Observatoire
de la sécurité des flux
et des matières énergétiques

Rapport

LE RÉSEAU DE TRANSPORT ÉLECTRIQUE EUROPÉEN ET SES ENJEUX DE SÉCURITÉ

Octobre 2024

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Enerdata
intelligence + consulting

CASSINI

DGRIS

Observatoire
de la sécurité des flux
et des matières énergétiques

L'Observatoire de la sécurité des flux et des matières énergétiques est coordonné par l'IRIS, en consortium avec Enerdata et Cassini, dans le cadre d'un contrat avec la Direction générale des relations internationales et de la stratégie (DGRIS) du ministère des Armées. Il consiste à analyser les stratégies énergétiques de trois acteurs déterminants : la Chine, les États-Unis et la Russie.

Le consortium vise également à proposer une vision géopolitique des enjeux énergétiques, en lien avec les enjeux de défense et de sécurité ; croiser les approches : géopolitique, économique et sectorielle ; s'appuyer sur la complémentarité des outils : analyse qualitative, données économiques et énergétiques, cartographie interactive ; réunir différents réseaux : académique, expertise, public, privé.

www.iris-france.org

Le ministère des Armées fait régulièrement appel à des études externalisées auprès d'instituts de recherche privés, selon une approche géographique ou sectorielle venant compléter son expertise externe. Ces relations contractuelles s'inscrivent dans le développement de la démarche prospective de défense, qui, comme le souligne le dernier Livre blanc sur la défense et la sécurité nationale, *« soit pouvoir s'appuyer sur une réflexion stratégique indépendante, pluridisciplinaire, originale, intégrant la recherche universitaire comme des instituts spécialisés »*.

Une grande partie de ces études sont rendues publiques et mises à disposition sur le site du ministère des Armées. Dans le cas d'une étude publiée de manière parcellaire, la Direction générale des relations internationales et de la stratégie peut être contactée pour plus d'informations.

AVERTISSEMENT : Les propos énoncés dans les études et observatoires ne sauraient engager la responsabilité de la Direction générale des relations internationales et de la stratégie ou de l'organisme pilote de l'étude, pas plus qu'ils ne reflètent une prise de position officielle du ministère des Armées.

À PROPOS DE L'AUTRICE ET DES AUTEURS DU RAPPORT

Angélique Palle / Géographe et chercheuse associée, Institut national du service public (INSP)

Docteure en Géographie, chercheure associée à l'Institut national du service public et à l'Institut de recherche stratégique de l'École militaire.

Luca Baccarini / Chercheur associé, IRIS

Luca Baccarini est chercheur associé à l'IRIS. Il est spécialiste dans les relations entre marchés de l'énergie, finance et géopolitique.

Sami Ramdani / Chercheur, IRIS

Chercheur au sein du Programme Climat, Énergie et Sécurité à l'IRIS et coordinateur de l'Observatoire de la sécurité des flux et des matières énergétiques. Il s'est spécialisé sur la géopolitique de l'énergie et des matières premières.

RESPONSABLE SCIENTIFIQUE ET COORDINATEUR

Emmanuel Hache / Directeur de recherche, IRIS

Directeur de recherche à l'IRIS et responsable scientifique de l'Observatoire de la sécurité des flux et des matières énergétiques. Il s'est spécialisé sur les questions relatives à la prospective énergétique et à l'économie des ressources naturelles.

Sami Ramdani / Chercheur, IRIS

CARTOGRAPHES

David Amsellem / Directeur, Cassini

Docteur en géopolitique et directeur du cabinet CASSINI. Il est spécialisé sur les questions d'aménagement, de transport public et de gestion des ressources énergétiques, en particulier au Proche et au Moyen-Orient.

Esther Bourgeois / Analyste et cartographe, Cassini

Consultante et cartographe au sein du cabinet Cassini. Elle a travaillé dans le domaine de la Défense (IRSEM, CESM) ainsi que dans l'humanitaire (ONG), avant de prendre en charge le pôle cartographie au sein de Cassini.

TABLE DES MATIÈRES

INTRODUCTION

L'électricité est une composante vitale du mode d'organisation de nos sociétés : l'approvisionnement en eau, la conservation de la nourriture, l'ensemble de l'économie mondialisée et des modes de communications en dépendent. Les sociétés occidentales (on s'intéresse ici au cas de l'Union européenne (UE)) ont fait reposer leur approvisionnement en électricité sur des réseaux d'infrastructures qui assurent la production et la distribution de la ressource. Éléments stratégiques de la défense et de la sécurité nationale. Ils ont été et redeviennent depuis le début du 21e siècle des cibles physiques, notamment lors de conflits, et sont largement concernés par des menaces cyber. Ils jouent également un rôle crucial dans les dynamiques de transition énergétique en cours dans l'UE et font l'objet de profondes mutations techniques et de conception qui affectent leur vulnérabilité.

Ce rapport propose un état des lieux des risques qui pèsent sur les réseaux de transport d'électricité dans l'espace européen. S'agissant d'objets techniques particulièrement complexes dont la maîtrise des bases du fonctionnement est nécessaire à leur analyse géopolitique, cette introduction s'adresse principalement au lecteur non spécialiste du sujet et contient : un bref récapitulatif des bases techniques, de l'architecture électrique européenne, du fonctionnement de son marché et de ses enjeux historiques et géopolitiques ainsi qu'un état des lieux des facteurs de vulnérabilité identifiés de ces réseaux.

1. Éléments essentiels sur le fonctionnement du réseau électrique européen

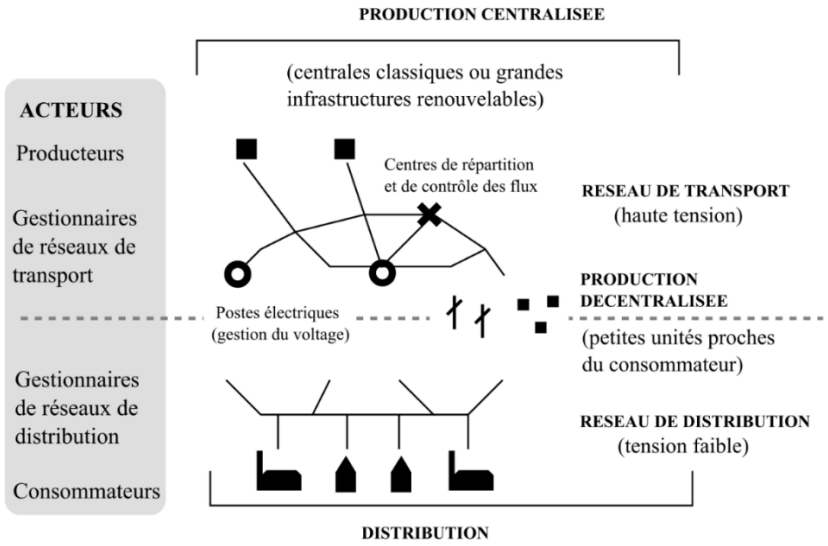
Bases techniques

Les deux schémas suivants présentent les caractéristiques de l'architecture du système électrique européen à la fois sur le plan technique et sur le plan institutionnel. Deux éléments majeurs sont à noter :

- Les pays de l'UE mènent depuis les années 1990 une politique d'intégration des réseaux et des marchés de l'énergie qui a conduit à développer très largement les interconnexions entre États. L'objectif actuel du secteur consiste à assurer leur développement de telle sorte que chaque État puisse échanger un minimum de 15% de sa production d'électricité avec ses voisins. Cette interconnexion et cette interdépendance des réseaux ont conduit à une multiplication des acteurs de niveau européens qui en assurent la gestion (schéma 2).
- La politique de transition énergétique menée par l'UE conduit à intégrer de nouvelles sources renouvelables de production d'électricité dont la nature ainsi que l'échelle modifient l'architecture du réseau de transport d'électricité européen. Il s'agit en effet d'une production intermittente et peu pilotable assurée à la fois par de grandes

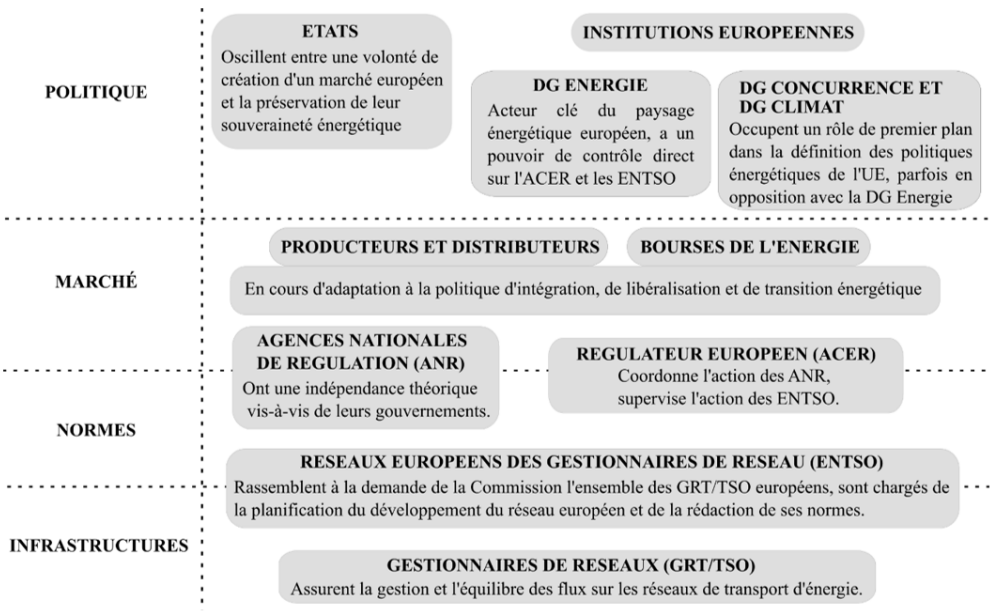
infrastructures de type parcs éoliens ou solaires mais aussi par de petites infrastructures individuelles intégrées dans le réseau de distribution plus que dans le réseau de transport (schéma 1)

Schéma 1 – Fonctionnement schématique d'un réseau électrique



Source : (Palle, 2016)[1]

Schéma 2 – Principaux acteurs de l'énergie dans l'Union européenne



Source : (Palle, 2016)[2]

[1] Angélique Palle, « L'espace énergétique européen : quelle (s) intégration (s) régionale (s)? : réseaux, normes, marchés, politiques, des intégrations à plusieurs échelles? ». *Diss. Paris 1*, (2016).
[2] *Ibid.*

Encadré 1 – Points techniques essentiels à la compréhension du fonctionnement des réseaux européens dans une dimension géopolitique

- Un courant électrique alternatif, soit l'immense majorité du réseau européen actuel, est caractérisé par sa fréquence (la rotation d'un alternateur). La fréquence du réseau doit être maintenue à chaque instant pour assurer l'approvisionnement. Cela implique : 1. des délais de réaction extrêmement rapides en cas d'incident, 2. des effets de « cascade » en cas d'incident dans un réseau largement interconnecté, comme celui de l'UE. Les normes européennes tentent de prévenir ces effets de cascade par la règle dite du N-1 qui implique que toute infrastructure du réseau doit être redondante au moins une fois. Autrement dit, il faut « perdre » au moins deux éléments du réseau pour que l'approvisionnement soit menacé.
- Un réseau dit « synchrone » est un réseau où le courant a la même fréquence. Pour l'utilisateur, changer de zone synchrone implique d'utiliser un adaptateur de prise pour le branchement des appareils, les échanges entres zones non synchrones nécessitent des adaptations techniques.
- Le trajet de l'électricité sur le réseau de transport est imprévisible (loi de Kirchhoff).

La construction électrique européenne et ses effets géopolitiques actuels

Les frontières de l'Europe électrique ne sont pas celles de l'Europe politique et l'association des gestionnaires de réseaux de transport d'électricité européens (ENTSO-E), qui gère le développement et l'interconnexion des marchés et des réseaux de l'électricité en Europe, comprend 39 membres représentant 35 pays. La Turquie en est membre observateur depuis 2016.

L'ENSTO-E comprend cinq zones synchrones (voir Carte 1), issues de l'histoire de la construction des réseaux : maîtrise progressive des câbles sous-marins et différences entre le réseau électrique de l'URSS et celui de l'UE en construction.

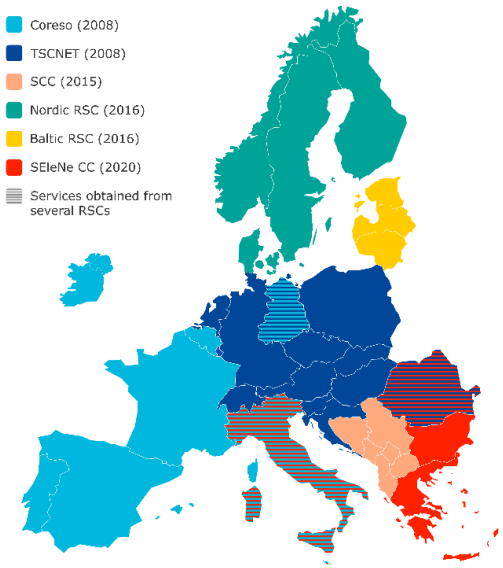
L'entrée des pays baltes dans l'UE en 2004 a ainsi été suivie d'importants investissements dans des interconnexions visant à les « débrancher » du réseau IPS/UPS de l'ex-URSS et à les raccorder aux réseaux et marchés européen pour limiter leur dépendance à la Russie.

Le maillage du réseau augmente la qualité de l'électricité, permet des économies d'échelle, des mécanismes de solidarité et une réduction de la dépendance aux importations extérieures, par diversification du mix et des sources d'approvisionnement. Il accroît cependant les « effets dominos » en cas d'incident. La croissance de l'interconnexion des

réseaux de transport d'électricité européens à partir des années 1990 a rapidement posé la question de la gestion des défaillances en cascades lors des incidents.

Le 4 novembre 2006, la déconnexion d'une ligne allemande déclenche un black-out qui affecte 15 millions de consommateurs européens dans 12 pays. L'incident a été aggravé par le comportement de la production décentralisée de parcs éoliens, dont la déconnexion et la reconnexion se sont faites de façon aléatoire. Il révèle à la fois la vulnérabilité du réseau européen interconnecté ainsi qu'un manque de coordination et de vision globale de son opération[3; 4; 5].

Carte 1 – Les centres de coordinations régionaux du réseau de transport d'électricité européen (2024)



Source : ENTSOE 2024[6]

Pour répondre à ces vulnérabilités, les gestionnaires de réseau nationaux et l'ENTSO-E mettent en place à partir de 2015 des centres de coordination régionaux, aujourd'hui obligatoires. Ils alertent, conseillent et forment les gestionnaires nationaux sur les mesures à prendre dans le contexte d'un réseau interconnecté à l'échelle européenne (voir Carte 2).

[3] UCTE, « Final Report », *System Disturbance on 4th November 2006* (Brussels: UCTE, 2007).
[4] CRE, *Rapport d'enquête de la Commission de régulation de l'énergie sur la panne d'électricité du samedi 4 novembre 2006* (Paris : 2007).
[5] ERGEG, « Rapport final », Les enseignements à tirer de la panne d'électricité du 4 novembre 2006 en Europe (Bruxelles : ERGEG, 2007).
[6] ENTSO-E, « Interconnected Europe », https://www.entsoe.eu/regions/ (page consultée le 10 juillet 2024).

Le dernier incident (4 juin 2024) qui a touché la Croatie, la Bosnie, le Monténégro et l'Albanie a ainsi été rapidement isolé du reste du réseau et a pu être résorbé en quelques heures[7].

Architecture et évolution du marché de l'électricité européen

En parallèle avec le développement des réseaux électriques, des interconnexions et de la génération renouvelable, l'UE sous l'impulsion de la Commission s'est engagée depuis la fin du siècle dernier dans un processus d'ouverture des marchés de l'électricité. Ce processus répond à des logiques libérales et concurrentielles et se décline sur les marchés de détails (suppression des monopoles et possibilité pour les consommateurs de faire appel à plusieurs fournisseurs) et sur les marchés de gros.

Le fonctionnement des marchés de gros de l'électricité est entrelacé avec la gestion des interconnexions et avec la sécurité de l'ensemble du système électrique. Le marché de l'électricité de gros européen se compose de différents marchés zonaux (dans la plupart des cas une zone = un pays) et de différents segments en fonction des maturités :

- Marchés à terme (avec des maturités jusqu'à plusieurs années) : produits échangés par le biais de contrats de gré à gré entre opérateurs (*over-the-counter*, *OTC*) ou via des bourses comme EEX[8].
- Marchés au comptant (*Spot*), opérés par des bourses de l'électricité : les échanges physiques de l'électricité ont lieu un jour (*Day-Ahead*) ou quelques minutes (*Intraday*) avant la livraison physique.
- Marchés d'équilibrage et mécanismes de réserve, opérés par les gestionnaires de réseaux pour les échanges d'énergie dans des délais très courts.

Chaque pays a ses propres infrastructures de marché, mais il faut noter la position dominante détenue par la bourse allemande EEX (filiale de Deutsche Börse) sur les marchés à terme et de la bourse EPEX SPOT (filiale de EEX Group) sur les échanges Day-Ahead.

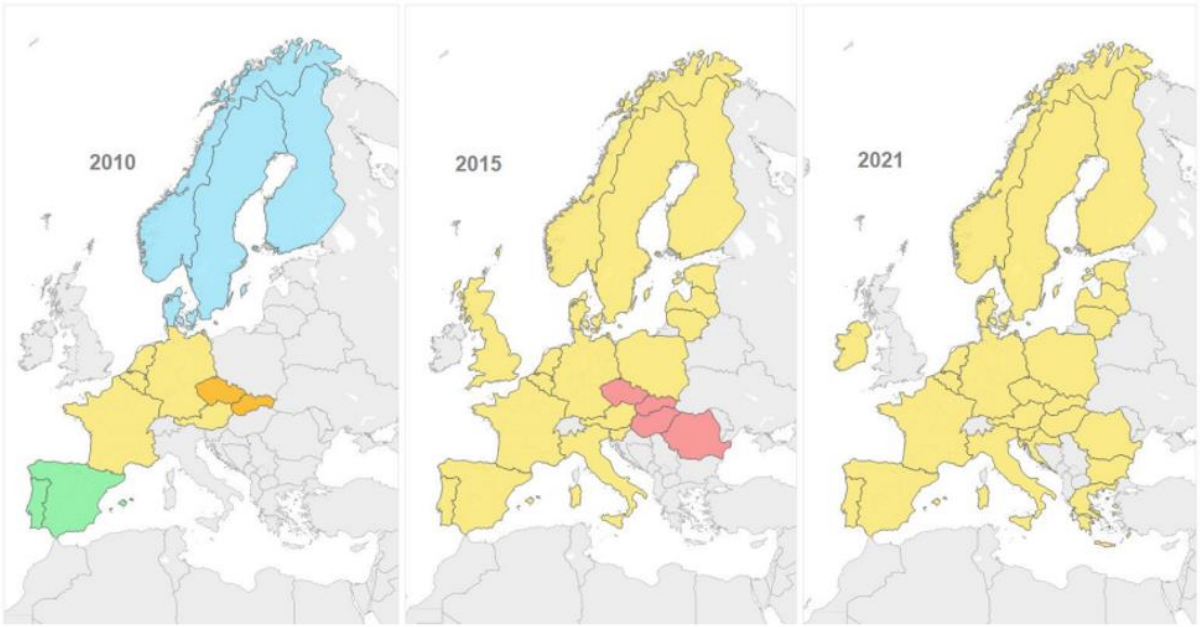
Les interconnexions – qui sont mises à disposition des acteurs de marché via des enchères - participent à l'établissement des prix sur les marchés, grâce au couplage des marchés (*Market Coupling*), qui consiste en un processus de mutualisation des offres et des demandes entre différentes zones de prix, dans la limite des capacités d'interconnexion entre ces zones. Lorsque ces capacités ne sont pas saturées (c'est-à-dire que la puissance du flux transitant aux interconnexions est inférieure à la capacité physique de ces dernières), le couplage des

[7] « Grid incident in south-eastern part of the Continental Europe power system », ENTSO-E, 15 July 2024.
[8] L'European Energy Exchange (EEX) est une des principales bourses de l'énergie européennes. Elle fait partie du groupe EEX, qui propose des contrats sur l'électricité, le gaz naturel et les quotas d'émission, ainsi que sur le fret et les produits agricoles. EEX fournit également des services de registre ainsi que des ventes aux enchères pour les garanties d'origine, pour le compte de l'État français.

marchés spot conduit à un prix commun pour l'ensemble des zones de prix interconnectées. Pour opérer ces échanges, les gestionnaires et bourses d'électricité sont associés : les premiers mettent à disposition des acteurs de marché les capacités d'échange entre les pays et gèrent le transit de l'électricité aux frontières, les seconds organisent la mutualisation des offres d'achat et de vente. Il en résulte des avantages économiques (la demande européenne est satisfaite à un coût de production moindre que si les marchés des États membres n'étaient pas connectés les uns aux autres) et une sécurité énergétique renforcée (les marchés peuvent s'appuyer les uns sur les autres en cas de pénurie d'approvisionnement ou de perturbations inattendues, renforçant ainsi la sécurité énergétique en réduisant la dépendance à une seule source ou d'un seul fournisseur d'énergie).

Le marché français a été d'abord couplé avec le Benelux en 2006, puis en 2010 avec l'Allemagne. En 2014/2015, le couplage a été étendu à la Grande-Bretagne, à l'Espagne, et à l'Italie. Les marchés sont désormais couplés dans 26 pays.

Carte 2 – Évolution du couplage des marchés de gros journalier de l'électricité dans l'UE (2010 - 2021)



Source : ACER, 2022[9]

[9] ACER, *Final Assessment of the EU Wholesale Electricity Market Design April 2022* (Ljubljana: ACER, 2022).

2. Facteurs et évolutions de la vulnérabilité des réseaux électriques européens

De nouvelles cibles pour les conflits hybrides, asymétriques ou de haute intensité

Plusieurs évolutions touchent les réseaux européens de transport d'électricité depuis le début des années 2000. Ces réseaux ont été des objectifs de guerre et protégés comme tels pendant la Deuxième Guerre mondiale[10], puis des éléments stratégiques de la reconstruction européenne après le conflit ainsi que pendant la guerre froide[11]. À partir des années 1990, l'accroissement des conflits asymétriques et les modes d'action, notamment terroristes, qui les caractérisent ont renforcé et changé les menaces potentielles pesant sur ces réseaux. Après les attentats du 11 septembre 2001, les États-Unis, l'UE et ses États membres ont progressivement repensé leur approche de la protection des infrastructures critiques dont font partie ces réseaux. Dans le contexte du conflit russo-ukrainien, les attaques menées contre le réseau ukrainien à l'hiver 2015, ainsi que les intrusions dans les réseaux de plusieurs États membres de l'OTAN, ont ravivé l'intérêt des États pour ces infrastructures, tandis que les campagnes de frappes russes sur les infrastructures électriques ukrainiennes depuis l'invasion du 24 février 2022 ont remis les réseaux de transport d'électricité au cœur des préoccupations de la résilience nationale.

Transition énergétique et numérisation changent le contexte de vulnérabilité des réseaux européens

Si le caractère asymétrique des conflits actuels et les modes d'action terroristes qu'ils génèrent ont transformé les menaces qui pèsent sur les réseaux d'électricité, le contexte dans lequel s'inscrit la gestion de ces réseaux a également beaucoup évolué depuis le début des années 2000. Dans l'UE, intégration des réseaux et transition énergétique ont ouvert de nouvelles vulnérabilités.

La politique énergétique de l'UE telle que définie par le traité de Lisbonne (Art. 194) promeut une intégration des réseaux d'énergie, à la fois pour permettre la mise en place d'un marché commun et pour réaliser des économies d'échelles. Cette interconnexion des systèmes de transport d'électricité accroît aussi les effets de cascade et de propagation en cas d'incident. Cela rend aujourd'hui impossible une approche uniquement nationale de leur protection. Le

[10] Henri Morsel, « Industrie électrique et défense en France lors des deux conflits mondiaux. Electricité, armement, défense. », *Bulletin d'histoire de l'électricité*, nº 23 (1994): 7-17.
[11] Vincent Lagendijk, *Electrifying Europe: The Power of Europe in the Construction of Electricity Networks* (Amsterdam: Amsterdam University Press, 2008).

réseau européen interconnecté[12] rassemble aujourd'hui 39 gestionnaires de réseaux qui doivent interagir pour assurer la sécurité d'approvisionnement de l'espace européen.

À cette vulnérabilité liée à l'interconnexion s'ajoute celle de l'ouverture des réseaux au numérique, dont le but est d'accroître l'efficacité énergétique[13] et l'optimisation technique en faisant circuler sur celui-ci, outre de l'électricité, de l'information en temps réel dans les deux sens. Cette politique entraine par exemple, de façon plus ou moins consciente et volontaire, la connexion de certaines infrastructures à internet ce qui les rend vulnérables au *hacking*[14].

La criticité des infrastructures électriques européennes et sa dimension politique

La sécurité des réseaux et du système électrique européen ne relève pas de questions strictement techniques. À l'échelon politique, la définition des critères de sécurité ou sûreté du réseau sont fonction du niveau d'investissement que la société est prête à consentir, pour protéger des intérêts qui sont à la fois économiques, sociaux et de défense. La protection absolue n'existe pas et un niveau de protection trop élevé par rapport à la probabilité d'un événement ou l'ampleur de ses conséquences, constitue un coût économique et social dans un contexte où le prix de l'énergie est un sujet particulièrement sensible politiquement.

La définition du niveau de vulnérabilité acceptable et la résilience (c'est-à-dire le temps et le coût d'un retour à la normale) attendue du réseau en cas d'incident ne peuvent alors être laissées à la seule appréciation des gestionnaires du réseau ou des entreprises du secteur électrique. Cela nécessite à la fois une prise de conscience et une prise de responsabilité des pouvoirs politiques, ainsi qu'une sensibilisation des consommateurs.

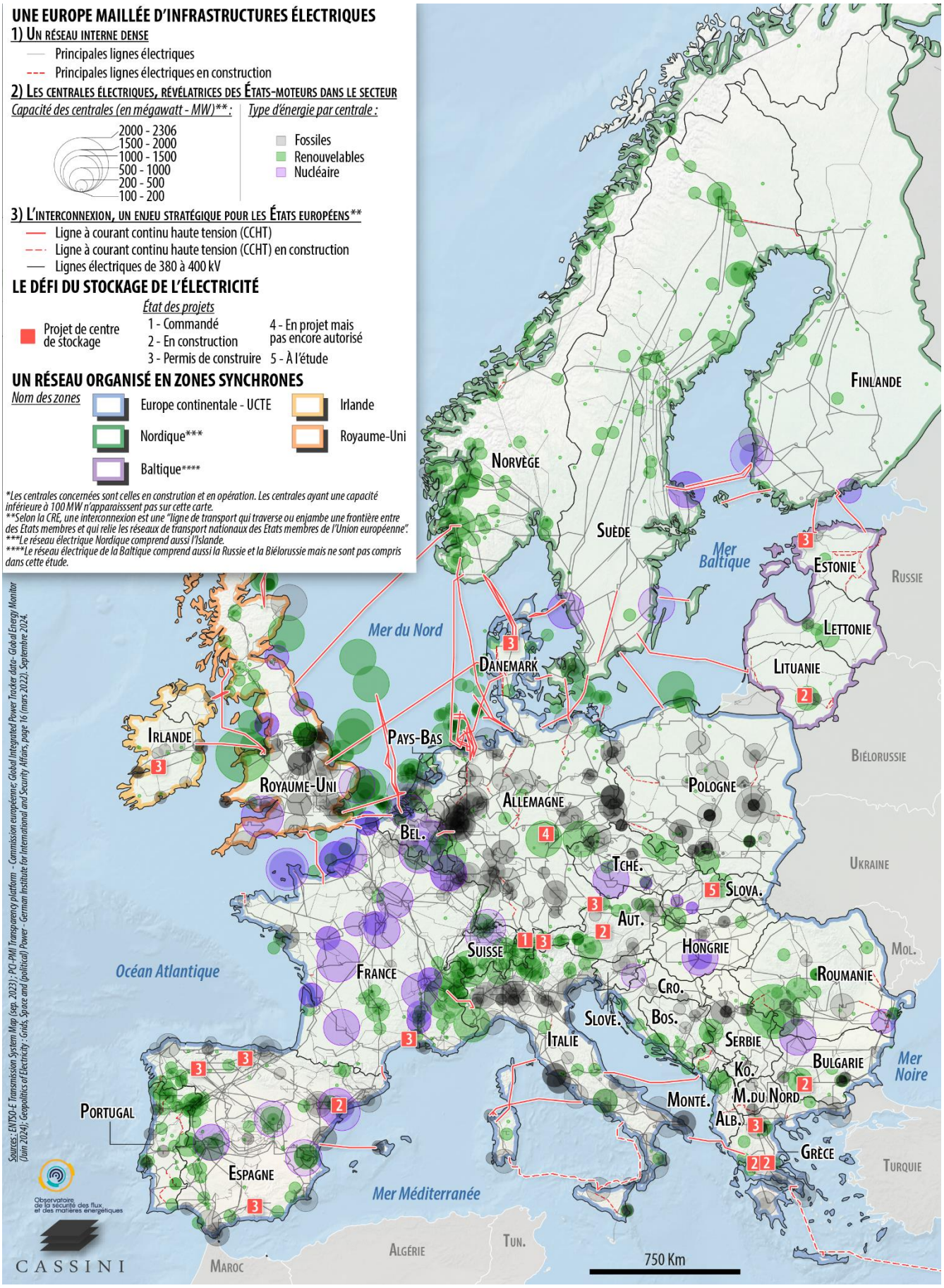
L'opération des marchés d'électricité de la plaque européenne est de plus en plus centralisée au niveau européen. Cette interdépendance *de facto* pose la question de la coordination et de l'échange d'information à l'échelle européenne pour la sûreté du réseau, et ce alors même que cette interconnexion ne concerne pas uniquement des pays membres de l'UE. La Suisse, la Norvège la Serbie, la Bosnie-Herzégovine, le Kosovo, le Monténégro, la Macédoine, le Royaume-Uni ou la Turquie sont interconnectés avec les différents réseaux synchrones européens et ne peuvent donc pas être laissés en dehors du champ de la coopération technique et de sécurité, sous peine de fragiliser l'ensemble.

[12] Il s'étend hors des frontières de l'UE et intègre notamment la Suisse, la Norvège, le Royaume-Uni, les pays de la péninsule balkanique mais aussi l'Ukraine.
[13] L'efficacité énergétique, utilisée au sens large du terme, désigne l'ensemble des technologies et pratiques qui permettent de diminuer la consommation d'énergie tout en conservant le même service final.
[14] « Smarter protection for the smart grid », *Mc Afee* (2012).

Objectifs et structure du rapport

Dans ce contexte, le présent rapport propose une analyse des enjeux de sécurité des réseaux électriques européens, en se plaçant notamment dans le contexte des effets du changement climatique et des politiques de transition énergétique européennes, ainsi que du conflit russo-ukrainien. Il propose dans un premier temps une analyse de la vulnérabilité et de la protection des réseaux de transport d'électricité européens avant d'aborder dans un second temps la résilience des infrastructures et des populations. La troisième partie propose un cas d'étude centré sur la résistance du réseau électrique ukrainien face aux campagnes de frappes russes et les enseignements possibles pour les réseaux européens. La conclusion propose à la fois des recommandations spécifiques au secteur de la défense et des éléments de comparaison internationales.

Carte 3 – Un réseau électrique européen connecté



VULNÉRABILITÉ ET PROTECTION DES RÉSEAUX DE TRANSPORT D'ÉLECTRICITÉ EUROPÉENS

1. Méthodologie : Aléas et vulnérabilité tendanciels des réseaux

On entend dans ce rapport la notion de risque telle qu'elle est utilisée et définie par les géographes et les aménageurs travaillant sur les risques naturels, industriels ou sociétaux [15;16]. Le risque est, dans ce champ, fonction de trois composantes :

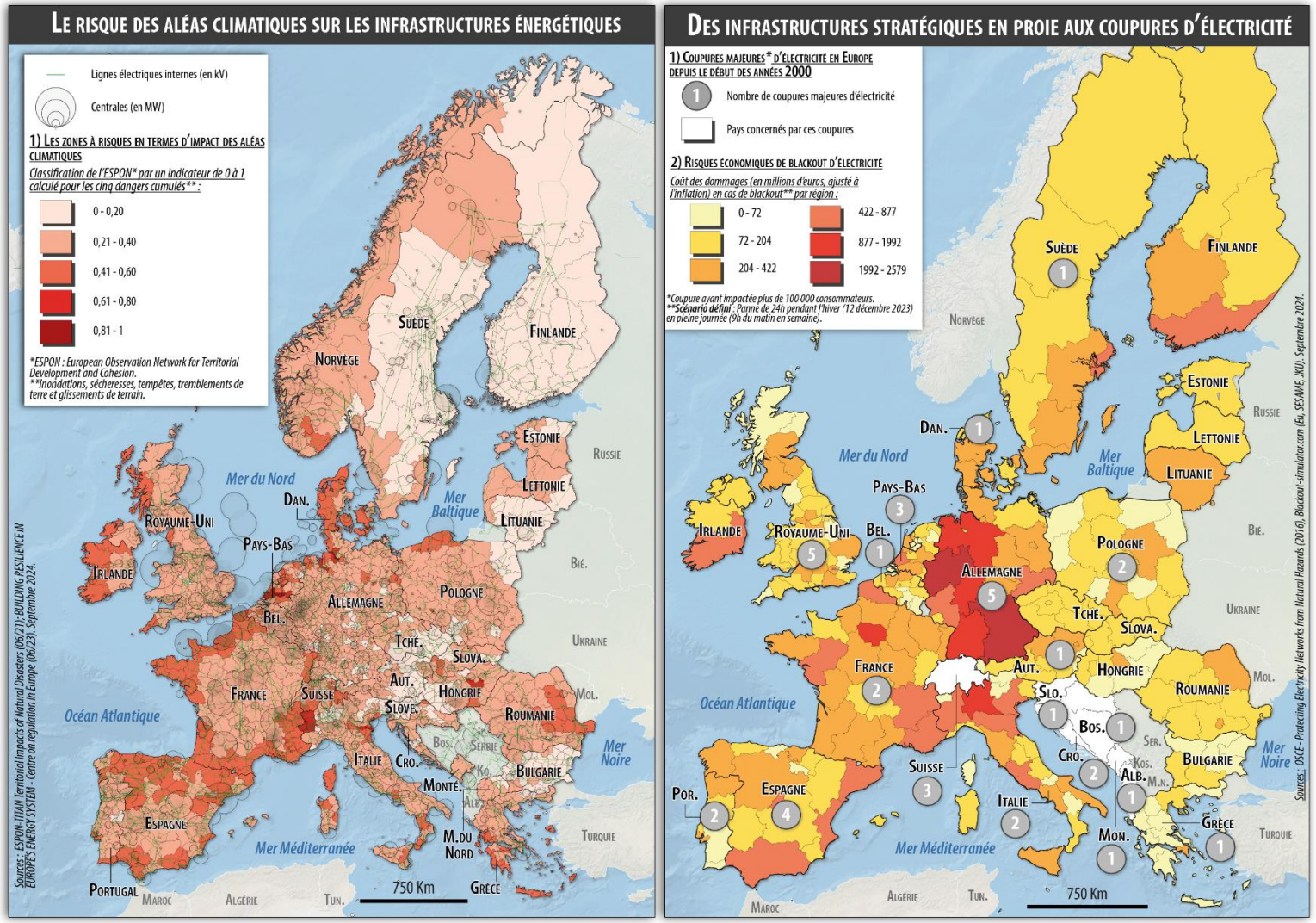
- L'aléa qui est la probabilité d'occurrence d'un événement (événement climatique, incident technique, attaque cyber ou physique etc.).
- La vulnérabilité qui est la propension d'un enjeu matériel ou humain considéré à être affecté par cet aléa (maillage du réseau, connexion à internet, câbles enterrés ou non).
- La résilience des infrastructures et des populations qui sont leur capacité à se régénérer dans un temps donné pour atteindre éventuellement un retour à la situation initiale. (Partie 2).

La paix et la construction européenne ont fait perdre aux réseaux de transport d'électricité la dimension stratégique et militaire qu'ils avaient acquis lors des deux Guerre mondiales et de la Guerre froide. Cette dimension stratégique au sens politique et militaire du terme est réactivée aujourd'hui à la fois à travers le conflit russo-ukrainien, face à des actions de sabotage ou de *hacking* issues de conflits asymétriques, d'oppositions politiques ou d'acteurs isolés, mais aussi dans le cadre des effets du changement climatique désormais perceptibles en Europe, notamment à travers d'événement climatiques extrêmes qui affectent le réseau.

À ces aléas s'ajoutent des vulnérabilités spécifiques à la politique de transition énergétique en cours dans l'UE. La part des énergies renouvelables dans le mix énergétique européen est en 2024 autour de 23%, elle doit doubler d'ici 2030 pour atteindre les objectifs que s'est fixée l'UE en matière de décarbonation. Le secteur électrique est en première ligne de cette politique avec à la fois une importante électrification des usages et un impératif d'intégration de sources d'énergie renouvelables. Cette production renouvelable, souvent intermittente et liée à la météo est difficilement pilotable. Son intégration au système électrique européen implique un renforcement du réseau et de ses interconnexions à la fois pour absorber l'intermittence des énergies renouvelables dans un contexte où le stockage de l'électricité demeure un enjeu technique et pour permettre des économies d'échelles et des complémentarités entre pays alors que l'électrification des usages est en croissance.

[15] Magali Reghezza et Yvette Veyret, « Vulnérabilité et risques. L'approche récente de la vulnérabilité », *Annales des mines*, n°43 (juillet 2006) : 9-13.
[16] Magali Reghezza-Zitt et Samuel Rufat (dir.), *Résiliences: sociétés et territoires face à l'incertitude, aux risques et aux catastrophes* (Londres: ISTE éditions, 2015).

Carte 4 – Les vulnérabilités de ce réseau électrique européen



2. La protection des réseaux redevient un enjeu

Les États européens, notamment l'Allemagne, la Belgique, la France, les Pays-Bas et l'Italie, se sont préparés à la Seconde Guerre mondiale en intégrant leurs réseaux électriques, ainsi que les centres de contrôle et de dispatching associés, à l'échelle nationale[17]. L'objectif était à la fois de renforcer le réseau en cas de conflit et de lui permettre de soutenir un effort de guerre économique. En France, une police spéciale est créée pour surveiller et protéger les infrastructures électriques. Les Allemands ont fait de même pendant l'occupation et deux régiments ont été affectés à la protection de la ligne stratégique reliant Paris et le Massif central[18].

Pendant l'occupation, le système électrique a été particulièrement sujet au sabotage par la résistance française, le gouvernement de Vichy recense 277 actions menées contre le réseau électrique dans la région Nord entre novembre 1943 et avril 1944, et deux importantes missions clandestines, Joséphine B. et Armada, ont ciblé le réseau électrique[19; 20].

À la fin de la guerre, les restrictions, les bombardements et les sabotages ont pratiquement paralysé le réseau français de transport d'électricité à haute tension. Quant à la production, elle a chuté de 30 % entre 1939 et 1944. Les alliés ont alors fait du rétablissement de l'approvisionnement en électricité et de la réhabilitation des réseaux l'une de leurs priorités. Pendant les années de la guerre froide, les infrastructures d'approvisionnement en électricité sont restées un enjeu stratégique. La réparation de la centrale électrique de Berlin-Ouest, endommagée et partiellement démantelée par les troupes soviétiques, fut par exemple l'un des enjeux du pont aérien américain pendant le blocus soviétique de la ville jusqu'en mai 1949[21].

La fin de la Guerre froide et la construction européenne ont mis en veille le caractère stratégique de ces réseaux que l'UE a cherché à partir du début des années 1990 à intégrer progressivement à l'échelle européenne pour la construction du marché unique. Les infrastructures de transport d'électricité sont alors peu protégées, les postes électriques sont le plus souvent non enterrées (pour des raisons budgétaires et d'accessibilité), sont largement

[17] Vincent Lagendijk, « Histoire de l'idée d'un système européen de l'électricité : projet, progrès, persistance », *Annales historiques de l'électricité*, nº 6 (1 octobre 2008) : 57-79.
[18] Hervé Bongrain, « L'électricité au service de la Défense nationale », *Histoire générale de l'électricité en France. Tome troisième*, par Maurice Lévy-Leboyer et Henri Morsel, éd. par Association pour l'histoire de l'électricité en France (Paris: Fayard, 1994).
[19] Sébastien Albertelli, *Histoire du sabotage : de la CGT à la Résistance* (Paris: Perrin, 2016).
[20] La première est le premier succès important du Special Operation Executive en France, la seconde en 1943 marque le début d'une campagne de sabotage menée par la résistance en France pour éviter les bombardements massifs et la destruction par les Britanniques d'infrastructures stratégiques.
[21] Vincent Lagendijk, « Histoire de l'idée d'un système européen de l'électricité : projet, progrès, persistance », *Annales historiques de l'électricité*, n°6 (1 octobre 2008) : 57-79.

visibles et protégés par de simples grilles. Au milieu des années 2010, les gestionnaires de réseau de transport d'électricité européens se perçoivent comme des infrastructures « normales », sans dimension stratégique particulière.

Aux États-Unis, si le Department of Homeland Security (DHS), après les attentats du 11 septembre 2001, propose en 2006 un plan national de protection des infrastructures, aucune agence fédérale n'est officiellement en charge de la sécurité du réseau de transport d'électricité, ce vide législatif faisant reposer l'ensemble de la politique de sécurisation du réseau sur les seules initiatives de l'industrie de l'énergie[22]. L'attaque du poste électrique de Metcalf qui alimente la Silicon Valley en 2013 (cf. Encadré 2) met ce vide en évidence et conduit à la création la même année de l'Electricity Subsector Coordinating Council (ESCC). L'ESCC établit un lien direct entre le gouvernement fédéral et les industriels du secteur responsables de la protection du réseau. Le manque de coordination réelle à l'échelon fédéral pour la protection du réseau ainsi que l'absence de plan national de coordination avaient alors été pointés par le directeur de l'Agence fédérale de régulation de l'énergie américaine.

Encadré 2 – L'attaque du poste électrique de Metcalf (Silicon Valley) - 2013

Le 16 avril 2013, vers une heure du matin, le poste électrique Metcalf, située au sud-est de San José et qui gère l'alimentation en électricité de la Silicon Valley, est attaquée à l'AK-47. Après avoir coupé les fils du téléphone et de l'internet, le ou les assaillants mettent hors-service, en moins de 20 minutes, 17 transformateurs du poste. Celui-ci n'étant pas particulièrement stratégique pour le réseau, le black-out est évité, mais il faudra 27 jours de réparation et 15 millions de dollars pour remettre en état le matériel.

Les transformateurs ont pour fonction d'augmenter ou de diminuer le voltage des lignes, permettant ainsi d'atteindre les hautes tensions que demande le transport de l'électricité sur de longues distances. Longs à fabriquer (parfois plus de deux ans), ils peuvent coûter plusieurs millions d'euros et sont difficilement transportables. Lors de l'attaque du poste électrique Metcalf, les tireurs ont principalement endommagé les structures de refroidissement. Le fonctionnement du poste a pu être arrêté avant une surchauffe grave du matériel, ce qui a permis d'éviter de plus lourds dégâts.

Comme celui de Metcalf, les postes électriques sont la plupart du temps situés dans des zones peu habitées et sont peu protégées, souvent par de simples chaînes métalliques et des caméras. Il s'agit de prévenir le vol de matériel, principal risque

[22] MARTINEZ, Michael, « Sniper attack on Silicon Valley grid spurs security crusade by ex-regulator », *Cable News Network,* 8 février 2014.

encouru par ces infrastructures aujourd'hui. En l'occurrence, les caméras n'ont pas permis d'identifier le ou les tireurs, situés à l'extérieur du périmètre de surveillance. Un an après l'attaque, le même poste électrique faisait, en août 2014, l'objet d'un vol de matériel, sans que les systèmes d'alarme ne réagissent.

Sources : Foreign Policy 2013[23] *; NBC Bay Area 2014*[24]

3. De nouveaux aléas pour la protection physique des réseaux

La protection physique des réseaux de transport d'électricité est redevenue un enjeu aujourd'hui. Les enjeux de transition énergétique et de réponse au changement climatique les ont remises au centre d'une attention médiatique et ces infrastructures font l'objet de tentatives de sabotages régulières, particulièrement venant de groupes se réclamant d'une écologie radicale (cf. encadré ci-dessous).

Encadré 3 – Attaques physiques récentes contre le réseau d'électricité français (plaintes déposées par le gestionnaire du réseau RTE)

14 juillet 2021. Lachapelle-sous-Aubenas (Ardèche), plusieurs départs de feu dans un poste électrique de RTE sont revendiqués par un mouvement proche de la mouvance libertaire. Ils n'entrainent pas de coupure d'électricité.

18 décembre 2022. Saint-Just-et-Vacquières (Gard). Des militants écologistes revendiquent avoir tenté de scier un pylône supportant une ligne à très haute tension. Le site chimique de Salindres est visé.

11 avril 2023. Genas, dans l'est de la métropole de Lyon. Un incendie volontaire revendiqué par un groupe se réclamant de la mouvance écoradicale endommage une ligne haute tension, privant momentanément 7000 clients d'électricité ainsi que plusieurs fournisseurs de l'industrie nucléaire et de l'armement.

Les aléas physiques auxquels sont soumis ces réseaux proviennent également de la croissance des événements climatiques extrêmes issus du changement climatique. Aux États-Unis, ces derniers font l'objet de groupes dédiés de l'Electricity Subsector Coordinating Council (ESCC), l'organisme de liaison entre le gouvernement fédéral et le secteur de l'électricité : après l'ouragan Sandy en 2012, l'ESCC et le Department of Energy ont établi un processus de

[23] Shane Harris, « "Military-Style" Raid on California Power Station Spooks U.S », *Foreign Policy,* 27 décembre 2013.
[24] Joe Jr. Rosato, « Following Attack on PG&E Substation, Bill Requires California Utilities to Beef Up Security », *NBC Bay Area,* 10 mars 2014.

réponse coordonné aux catastrophes environnementales pour le secteur électrique. Les grands incendies qui touchent désormais régulièrement la côte Ouest des États-Unis font eux l'objet d'un groupe de travail dédié en partenariat avec l'U.S. Forest Service et le Bureau of Land Management, pour améliorer la détection des feux, élaborer les stratégies de gestion des terres du secteur, et répondre aux urgences liées aux incendies de forêt[25].

Dans l'UE, le règlement (EU) 2019/941 sur la préparation aux risques dans le secteur de l'électricité, impose aux États membres de mettre en place des mesures pour prévenir, se préparer à et gérer les possibles crises affectant le secteur électrique. Son article 6 charge l'ENTSOE, le réseau européen des gestionnaires de réseaux de transport d'électricité, d'identifier les scénarios de crise électriques les plus probables à une échelle régionale. Les scénarios sont mis à jour tous les quatre ans (la seconde itération de ces scénarios a été remise en 2024)[26]. L'ENTSO-E n'organise pas d'exercice de gestion de crise spécifique à son niveau. Certains États de l'UE, seuls ou en groupes, effectuent des exercices à plusieurs échelles, c'est le cas des membres du Forum Pentalatéral[27].

Ces aléas physiques interviennent dans un contexte industriel particulier : si les technologies nécessaires à l'entretien et la réparation de ces infrastructures sont aujourd'hui largement disponibles à la fois sur le plan matériel et logiciel, les industriels et gestionnaires de réseaux européens et américains alertent sur « de sérieux goulets d'étranglement en matière de capacité de fabrication et de ressources qualifiées »[28]. Le Département de l'énergie américain a publié en 2023 un recensement des points chauds de la chaine de valeur énergétique, dans le domaine de la transmission. Ils concernent principalement : pour les matières premières l'étape de la transformation, pour la fabrication et l'assemblage les étapes d'assemblages intermédiaires et finales, et pour la main d'œuvre l'opération des infrastructures installées[29].

4. Gérer la recrudescence des cyberattaques

Le secteur du transport d'électricité européen a dû ouvrir ses infrastructures au numérique pour gérer le pilotage de la production renouvelable. En France, par exemple, les nouveaux postes électriques à haute et très haute tension déployés par RTE le gestionnaire du réseau de transport d'électricité sont équipés de fibre optique et de capteurs pour mesurer en temps

[25] Electricity Subsector Coordinating Council, « Protecting the energy grid from national-level disasters and threats is a responsibility the government and the electric power industry share », 2024 https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure
[26] L'identification et le classement de ces scénarios sont effectués selon une méthode développée par l'ENTSO-E et l'ACER en 2024 "Methodology for Identifying Regional Electricity Crisis Scenarios".
[27] Le Forum pentalatéral de l'énergie est une structure de coopération régionale entre la Belgique, les Pays-Bas, le Luxembourg, l'Allemagne, la France, l'Autriche et la Suisse.
[28] Future of our Grids, *Discussion and Conclusions of the High-Level Forum*, Brussels, 7 September 2023.
[29] US Department of Energy, *Supply Chains Progress Report* (Washington : DOE, 2023).

réel les flux et recueillir les données utiles pour gérer de manière dynamique le système électrique permettant ainsi d'intégrer jusqu'à 30 % d'électricité supplémentaire issue de sources renouvelables. La cybersécurité est alors une préoccupation croissante pour les infrastructures énergétiques de l'UE. En 2023, plus de 200 cyber incidents signalés ont visé le secteur de l'énergie et plus de la moitié d'entre eux ont été dirigés spécifiquement contre l'Europe (source ENISA).

Encadré 4 – Des attaques cyber reconnues depuis la fin des années 2010

Ukraine – 2015[30]

Le 23 décembre 2015, un black-out en Ukraine touche environ 225 000 consommateurs, il est attribué à une cyber attaque perpétrée contre le réseau de transport d'électricité. L'attaque aurait ciblé les systèmes de contrôle des infrastructures du réseau mais aussi de façon directe sept sous-stations dont les opérateurs du réseau n'ont pas pu reprendre le contrôle et qui ont nécessité l'envoi d'équipes de maintenance pour effectuer des réparations sur les sous-stations touchées. Les lignes de téléphone des opérateurs ont également été brouillées. L'attaque a été attribuée par l'Ukraine à la Russie avec laquelle elle se trouve alors en conflit ouvert depuis plus d'un an. Il s'agit de la première cyberattaque contre un réseau électrique officiellement reconnue comme « réussie ».

Cyber attaque « Berserk Bears » (Allemagne) – Printemps 2018

Le 20 mai 2018, le directeur de l'Office fédéral de protection de la Constitution (le service de renseignement intérieur allemand), après plusieurs alertes de l'Office fédéral pour la sécurité informatique, accuse publiquement la Russie de mener une campagne d'infiltration informatique visant le secteur de l'énergie allemand, notamment les fournisseurs d'électricité. Deux mois auparavant, les États-Unis avaient également dénoncé une campagne de cyber attaques visant leur réseau d'électricité et désigné la Russie comme responsable.

L'interdépendance croissante entre technologies de l'information et de la communication (TIC) et secteur électrique ajoute au caractère critique de ce dernier. Les nombreux systèmes de pilotage par la donnée en cours de construction dans la plupart des secteurs allant de l'internet des objets aux *smart cities*, sont dépendant d'un approvisionnement électrique continu. Une perturbation de l'approvisionnement en électricité peut alors avoir un impact

[30] « Cyber-Attack Against Ukrainian Critical Infrastructure », US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, 25 February 2016.

majeur sur la société avec une cascade d'effets dans d'autres secteurs souvent non préparés à cette éventualité. Inversement, la déconcentration d'une partie de la production et du transport de l'électricité permise par les technologies *smart grids* permet aussi un phénomène de résilience des réseaux.

Encadré 5 – Scénario ENISA pour la croissance de la production renouvelable décentralisée

« L'intégration des énergies renouvelables et l'automatisation des équipements sont des tendances significatives dans le secteur de l'énergie, mais le passage à une production d'énergie décentralisée offre la possibilité de renforcer la résilience, de réduire les risques de cybersécurité et d'autonomiser les consommateurs d'ici à 2030. La production d'énergie décentralisée peut améliorer la résilience des systèmes énergétiques. Par exemple, en cas de catastrophe naturelle ou d'autres perturbations, les sources d'énergie locales peuvent continuer à fonctionner et à alimenter les infrastructures essentielles et les foyers. Si la décentralisation offre de nombreux avantages, il reste des défis à relever, tels que la gestion du réseau, le stockage de l'énergie et les cadres réglementaires. En outre, l'intégration continue des technologies de l'internet des objets (IoT) jouera un rôle essentiel dans la gestion efficace de ces systèmes énergétiques en évolution. »

Source : ENISA 2024 [31]

Selon le rapport *Network and Information Security (NIS) Investments in the EU* de l'Agence de l'Union européenne pour la cybersécurité (ENISA, 2023), 32% des opérateurs du secteur de l'énergie n'ont pas processus critique unique de technologie opérationnelle (OT) surveillé par un centre d'opérations de sécurité (SOC). Les technologies opérationnelles et les technologies de l'information sont couvertes par un seul SOC pour 52 % des opérateurs de services essentiels dans le secteur de l'énergie.

Dans un contexte de conflit de haute intensité entre l'Ukraine et la Russie, dans lequel la résilience du réseau de transport d'électricité ukrainien joue un rôle majeur et fait l'objet de campagnes de frappes régulières par la Russie, l'exercice Cyber Europe paneuropéen de juin 2024 organisé par l'ENISA s'est concentré sur un scénario impliquant des cybermenaces visant l'infrastructure énergétique de l'UE et découlant de frictions causées par des tensions géopolitiques entre l'Union européenne et une nation étrangère fictive. Il a réuni 30 agences

[31] ENISA, *Foresight cybersecurity threats for 2030 – Update 2024*, FORESIGHT CYBERSECURITY THREATS FOR 2030 – UPDATE (Athens: ENISA, 2024).

nationales de cybersécurité, des agences, organismes et réseaux de l'UE et plus de 1 000 experts traitant d'un éventail de domaines allant de la réponse à l'incident à la prise de décision. Si les compagnies européennes ont globalement bien tenu l'exercice, l'enjeu pour les parties prenantes a été de coordonner rapidement leurs actions et leurs réponses. La gestion de la dimension transfrontalière notamment et le partage des informations concernant la nature internationale ou non des incidents par les CSIRT (Computer Security Incident Response Teams) peut être améliorée. La nécessité d'approches régionales et de mise en place de procédures de transmission d'informations à cette échelle a été soulignée par l'ENISA lors de son retour d'expérience au 7th Cybersecurity forum organisé à Bruxelles le 1er octobre 2024. Le niveau de coordination actuelle est ainsi jugé insuffisant en cas d'incidents affectant simultanément plusieurs États.

Pour renforcer cette coordination à l'échelle européenne essentielle en cas d'incident cyber de grande envergure, plusieurs initiatives politiques sont en cours : le réseau européen des gestionnaires de transport d'électricité (ENTSO-E) a rédigé un code de réseau commun sur la cybersécurité. Entré en vigueur en juin 2024 il vise à établir une norme européenne pour la cybersécurité des flux transfrontaliers d'électricité. Il comprend des règles sur l'évaluation du risque cybernétique, des exigences minimales communes, la certification des produits et services en matière de cybersécurité, la surveillance, l'établissement de rapports et la gestion des crises. La DG Énergie dans le cadre de son groupe d'expert sur les énergies intelligentes cherche également à évaluer les ramifications des nouvelles initiatives législatives dans ce domaine. Chez les acteurs industriels, des centres de partage et d'analyse de l'information (ISAC) comme l'European Energy Information Sharing & Analysis Centre, voient également le jour à des échelles nationales ou européennes et structurent des flux d'informations sur l'évolution des menaces et la réponse aux cyberincidents.

5. Sécurité économique, gestion des investissements étrangers

La sécurité physique et cyber du réseau de transport d'électricité européen repose, pour les raisons évoquées dans les 2. et 3. précédents, sur des normes communes et un large partage d'informations entre acteurs du secteur. Ce partage d'informations inclut désormais des acteurs non membres de l'UE, à la fois du fait de la synchronisation des réseaux européens avec des pays voisins mais aussi du fait d'investissements de pays tiers dans ces réseaux de transport.

Le secteur énergétique est l'un des principaux secteurs dans lequel la Chine investit en Europe. En 2019, les secteurs du transport, de l'énergie des utilities et des infrastructures concentraient 800 millions d'euros d'investissements directs étrangers. Si ces investissements

ont diminué après 2019 du fait du covid et des tensions grandissantes entre la Chine et l'UE, le solaire photovoltaïque continue de tirer les investissements chinois en UE[32].

Dans le cadre de son projet des nouvelles routes de la soir et de sa stratégie de connectivité, la Chine a investi dans les réseaux de transport d'électricité européens lorsque cela s'est avéré possible. State Grid Corporation of China, le monopole d'État chinois sur le réseau de transport d'électricité et la société d'énergie la plus valorisée au monde (top 10 des plus grandes entreprises du monde), a multiplié les prises de participations dans les réseaux européens.

Encadré 6 – Prises de participations de State Grid Corporation of China dans les opérateurs de transport d'énergie européens

1. REN (Redes Energéticas Nacionais) – Portugal : En 2012, SGCC a acquis une participation de 25 % dans l'opérateur du réseau national d'énergie du Portugal, REN. Cet investissement s'inscrivait dans le cadre des efforts de privatisation du Portugal pendant la crise de la zone euro.

2. CDP Reti (Italie) - Participation dans Terna : En 2014, SGCC a acquis une participation de 35 % dans CDP Reti, une société holding italienne contrôlée par Cassa Depositi e Prestiti (CDP). Par l'intermédiaire de CDP Reti, la SGCC a acquis une exposition indirecte à Terna, le gestionnaire du réseau de transport d'électricité italien, qui est l'un des plus importants d'Europe. Terna possède et gère la majeure partie du réseau italien de transport d'électricité à haute tension.

3. ADMIE (Grèce) : En 2017, SGCC a acquis une part de 24% dans ADMIE le gestionnaire de transport d'électricité grec. Cet achat a lieu dans le cadre des opérations de privatisations conduites en Grèce suite à la crise financière auquel le pays fait face.

4. 50Hertz – Allemagne : En 2018, SGCC a fait une offre pour acquérir une participation de 20 % dans 50Hertz, l'un des quatre opérateurs de transport d'électricité en Allemagne. Cependant, le gouvernement allemand, invoquant des préoccupations stratégiques en matière de sécurité nationale et d'approvisionnement énergétique, est intervenu et a bloqué la vente en faisant en sorte que la banque de développement publique allemande KfW achète la participation à la place.

5. Groupe SGB-SMIT (Allemagne) : Bien qu'il ne soit pas un gestionnaire direct de réseau de transport, le groupe SGB-SMIT est un fabricant de transformateurs de

[32] Rhodium Group and MERICS, *Dwindling investments become more concentrated - Chinese FDI in Europe: 2023 Update* (Berlin: Mercator Institute for China Studies, 2024).

premier plan en Europe. En 2017, une filiale de SGCC a acquis une participation majoritaire dans cette entreprise allemande.

Sources : China Daily, Reuters, PingMagazine Asia.

L'ensemble de ces opérations et la présence de SGCC aux conseils d'administration de certaines de ces entreprises lui confèrent une visibilité sur la stratégie de développement des réseaux de transports d'électricité européens ainsi que sur leurs vulnérabilités.

RÉSILIENCE DES INFRASTRUCTURES, DES MARCHÉS ET DES POPULATIONS

Comment les évolutions de ces vulnérabilités du système électrique sont-elles prises en compte par les acteurs du secteur ? Cette partie rend compte des initiatives en matière de résilience, dont elle dresse un état des lieux pour les infrastructures, les marchés et les populations.

1. OTAN, UE, États voisins ou échelle nationale, à quel niveau faut-il gérer la résilience du réseau

La gestion de la résilience du réseau électrique est particulièrement complexe dans la mesure où cette infrastructure, critique pour la souveraineté nationale, fait l'objet d'une interconnexion européenne et d'échange d'informations qui s'étendent au-delà de ses alliances stratégiques. Cette question de la résilience et de sa gestion est alors prise en compte à plusieurs échelles, dont certaines sont en compétition.

Au sein de l'OTAN la notion de résilience est associée à l'Article 3 du Traité de l'Atlantique Nord « les parties, […] maintiendront et accroîtront leur capacité individuelle et collective de résistance à une attaque armée ». Les États-Unis y poussent la construction d'une notion de résilience nationale très large comprenant l'ensemble du fonctionnement des infrastructures critiques d'un pays mais aussi la cohésion nationale de sa population. Ces deux éléments conditionnent, la possibilité d'une opération militaire et d'un déploiement de troupes par et sur le territoire de l'État concerné. Cette construction américaine de la notion de résilience conduit les États-Unis à demander à leurs alliés d'évaluer l'état de leurs infrastructures, notamment énergétiques et de partager cette information. Cet investissement de la notion de résilience par les États-Unis dans le cadre de l'OTAN est notamment construit pour permettre de contrôler et de limiter le niveau d'investissement et d'accès chinois aux infrastructures des pays alliés.

Pour l'Union européenne la résilience entendue au sens large de capacité de gestion et de résistance aux crises recouvre à la fois des enjeux sanitaires, migratoires, de sécurité des infrastructures face à des risques environnementaux ou sécuritaires, ou de protection civile[33]. Dans le cas des réseaux de transport d'électricité, l'UE elle prend en compte le risque cyber à une échelle européenne avec les directives NIS, les exercices de l'ENISA et des codes de réseaux communs définis par l'ENTSO-E dont les normes cyber sont entrées en vigueur en 2024 et sont en cours de mise en œuvre. La sécurité des mécanismes de marché (cf. Partie 2.2) est également envisagée à une échelle européenne. La sécurité des flux physiques est construite à une échelle infrarégionale, qui rassemble des groupes d'États voisins au sein de

[33] Conseil de l'Union européenne, « Conclusions du conseil sur le renforcement de la préparation, de La capacite de réaction et de la résilience face aux crises à venir », 23 novembre 2021.

six coordinateurs régionaux de sécurité (cf. Introduction, Carte X.), tandis que la sécurité physique des infrastructures est prise en compte à une échelle nationale par les États.

Cette construction à plusieurs échelles de la sécurité des réseaux implique alors une très grande coordination des différents acteurs. L'étude du cas ukrainien (cf. Partie 3. 2.) montre en effet que dans le cas d'un ciblage spécifique des infrastructures électriques, la coordination d'attaques cyber et physiques est particulièrement efficace. Les États-Unis ont commencé à s'exercer à la gestion de cette double vulnérabilité à partir du milieu des années 2010 à travers les exercices Gridex[34]. Comparativement, l'UE manque encore d'exercices de grande envergure menés à l'échelle européenne et comprenant plusieurs dimensions de sécurité.

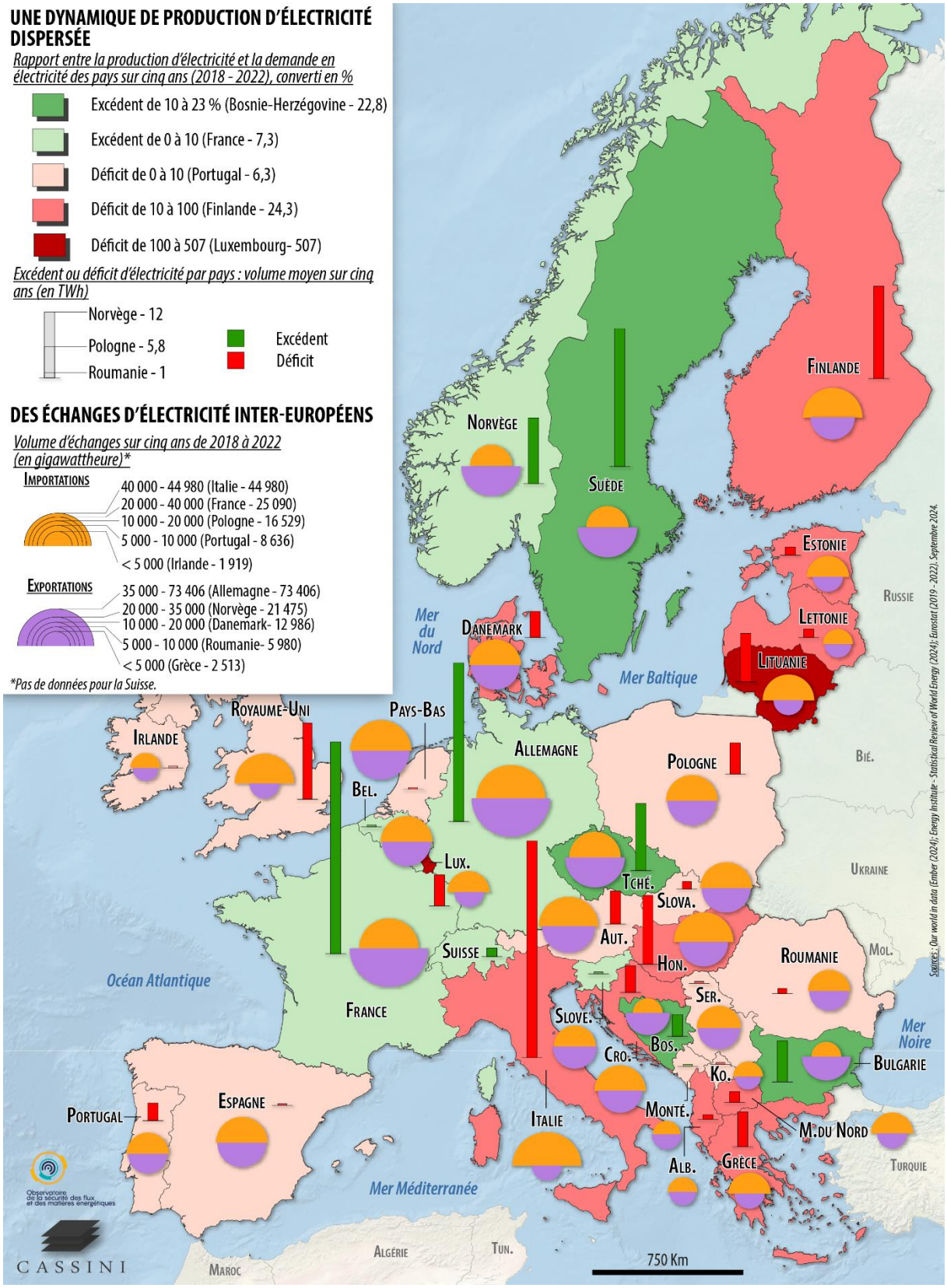
2. Résilience des marchés européens

Des avantages économiques et une sécurité énergétique renforcée résultent de l'interactions des différents marchés et de la mise à disposition de capacités d'interconnexion. Le concept de base est qu'une plus grande interconnexion des marchés permet d'atteindre des synergies croissantes, notamment dans un contexte de transition énergétique et de développement de la production renouvelable. Cette interconnexion permet une baisse des prix et des économies d'échelle. Les marchés interconnectés peuvent également s'appuyer les uns sur les autres en cas de pénurie d'approvisionnement ou de perturbations inattendues et réduire la dépendance à l'égard d'une seule source ou d'un seul fournisseur d'énergie.

Cependant, la croissante électrification de la consommation va conduire à une homogénéisation des comportements entre les différents pays. Dans le cas d'une forte corrélation des variabilités de certaines sources renouvelables (par exemple une faible pluviométrie au niveau continental), on pourrait assister à des déséquilibres régionaux entre la demande et l'offre d'électricité. Ces risques rendent donc souhaitable le maintien en activité de centrales électriques pilotables (par exemple des centrales à gaz naturel) ou le développement de nouvelles capacités de production bas-carbone et la croissance du stockage d'électricité pour compenser les déséquilibres entre l'offre et la demande. L'intégration des marchés signifie aussi qu'en cas d'incident les risques des effets de « cascade » et de propagation entre différentes zones augmentent.

[34] Angélique Palle, « Vulnérabilité et protection des réseaux électriques, Approches comparées Union européenne - États-Unis », *Notes 62*, IRSEM, (2018).

Carte 6 – Des équilibres de production et de consommation entre les pays européens



Il est nécessaire dans ce contexte de veiller à la résilience des organisations de marché face à des risques d'instabilité financière ou de manipulation, ainsi qu'à la résilience des marchés par rapport à des situations extrêmes, comme l'indisponibilité d'une partie des réseaux de transport d'électricité à la suite de catastrophes naturelles ou d'actes de sabotage.

Résilience des organisations de marché et systèmes de contrôle

Dans l'ensemble des marchés de l'électricité le rôle central est joué par les marchés au comptant (*Spot*), car sont ceux qui concentrent les échanges physiques. On distingue notamment les échanges physiques de l'électricité qui ont lieu un jour (*Day-Ahead*) ou quelques minutes (*Intraday*) avant la livraison physique. Les marchés Day-Ahead sont organisés par un système d'enchères tenues par les bourses d'électricité qui alignent une fois par jour les courbes d'offre et de demande (ordres d'achats et de ventes des différents acteurs ainsi que les capacités d'interconnexion disponibles), fixant ainsi un *clearing price*[35] unique pour chaque produit horaire avec livraison le lendemain. Les prix Day-Ahead sont aussi très importants car ils servent de base d'indexation pour des nombreuses transactions financières et des contrats de fourniture.

La solidité financière des bourses de l'électricité[36] est assurée par des mécanismes d'appels de marge et de garanties financières demandées aux acteurs de marché. L'ensemble de différentes couches de mesures, *reporting* et contrôles vise à assurer la sécurité des échanges sur les bourses, ce qui est fondamental pour protéger les acteurs de marchés et indirectement les consommateurs finaux aussi.

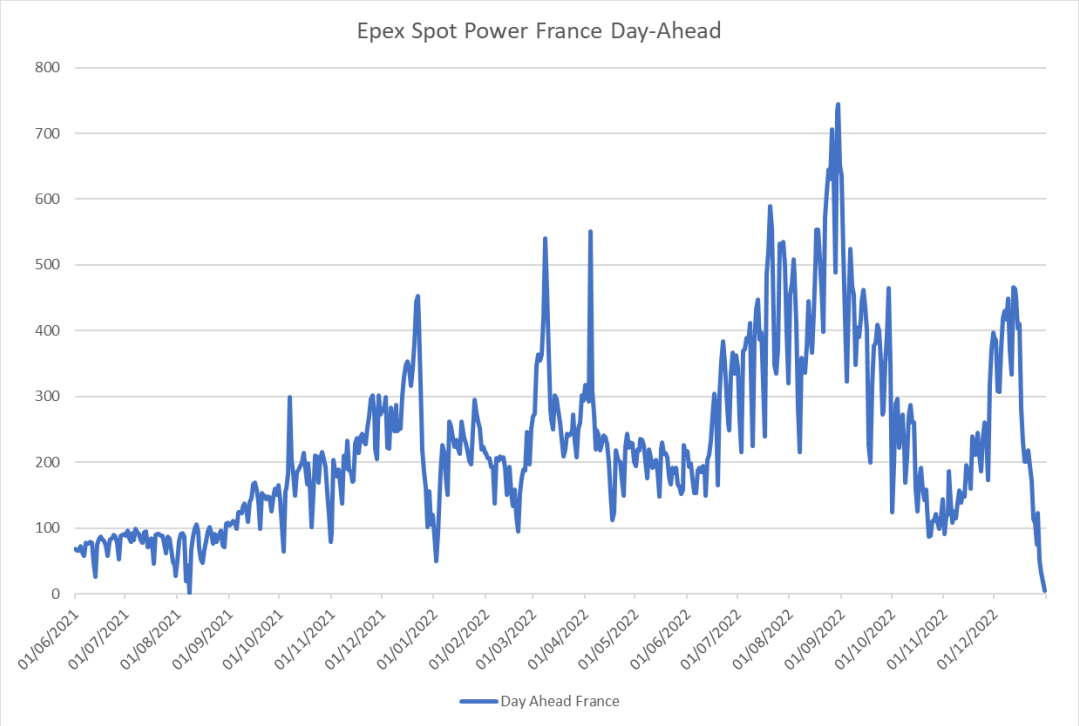
Encadré 7 – Focus sur la crise de l'énergie 2021-2022

À partir de l'été 2021 et pendant toute l'année 2022 les prix de l'électricité en Europe ont connu une très forte volatilité, avec des pointes de prix jamais enregistrées dans le passé.

Le graphique suivant montre l'évolution du prix du produit Power France Day-Ahead traité sur la bourse EPEX SPOT entre le 01/06/2021 et le 31/12/2022. Des comportements de prix similaires ont eu lieu sur les autres pays européens et pour les diverses maturités.

[35] Le *clearing price* résulte de la vérification des ordres passés sur le marché et de la compensation des différentes positions.
[36] Les bourses de l'électricité sont des entreprises financières soumises aux contrôles de l'ESMA (European Securities and Markets Authority), des autorités nationales comme l'AMF (Autorité des Marchés Financiers) et des agences nationales de régulation comme la CRE en France. De plus, les échanges font l'objet de suivis et déclarations dans le cadre de la REMIT (Regulation on Wholesale Energy Market Integrity and Transparency). La REMIT est un règlement de l'UE adopté en 2011 visant à établir une discipline commune sur tous les marchés européens de l'électricité, en augmentant la transparence et la stabilité, tout en luttant contre les délits d'initiés et les manipulations de marché.

Graphique 1 – Epex Spot Power France Day-Ahead



Source : Epex Power Spot, Day Ahead France.

La crise énergétique de 2021-2022 a été déclenchée par la conjonction de divers facteurs :

- L'invasion de l'Ukraine par la Russie en février 2022 – précédée par les manipulations des flux d'exportation et des prix du gaz de la part de Gazprom à partir de l'été 2021 - a posé un défi de taille aux marchés européens de l'énergie. Les prix exceptionnellement élevés du gaz ont fait grimper le coût des centrales électriques au gaz ;
- Le parc nucléaire français, un élément crucial du système électrique de l'Europe occidentale, a subi des opérations de maintenance sans précédent ;
- Une sécheresse record a entrainé une forte réduction de la production hydroélectrique.

Le système de marché a répondu à ces chocs en répartissant l'énergie rare sur un réseau européen contraint et en encourageant des réductions suffisantes de la demande. Les marchés intérieurs de l'électricité de l'UE ont été efficaces dans la mesure où ils ont permis un retour à l'équilibre. La France, par exemple, qui a été pendant des années un exportateur net massif d'électricité, est devenue bénéficiaire d'importantes importations d'électricité. Les prix élevés ont également contribué à faire baisser la demande sur le continent, tant pour l'électricité que pour le gaz. Dans

ce contexte extraordinairement tendu et volatil, les marchés de l'électricité ont continué à fonctionner de façon ordonnée. Un certain nombre d'acteurs de marché ont cependant connu des difficultés liées au financement de leurs appels de marges et aux besoins de garanties bancaires.

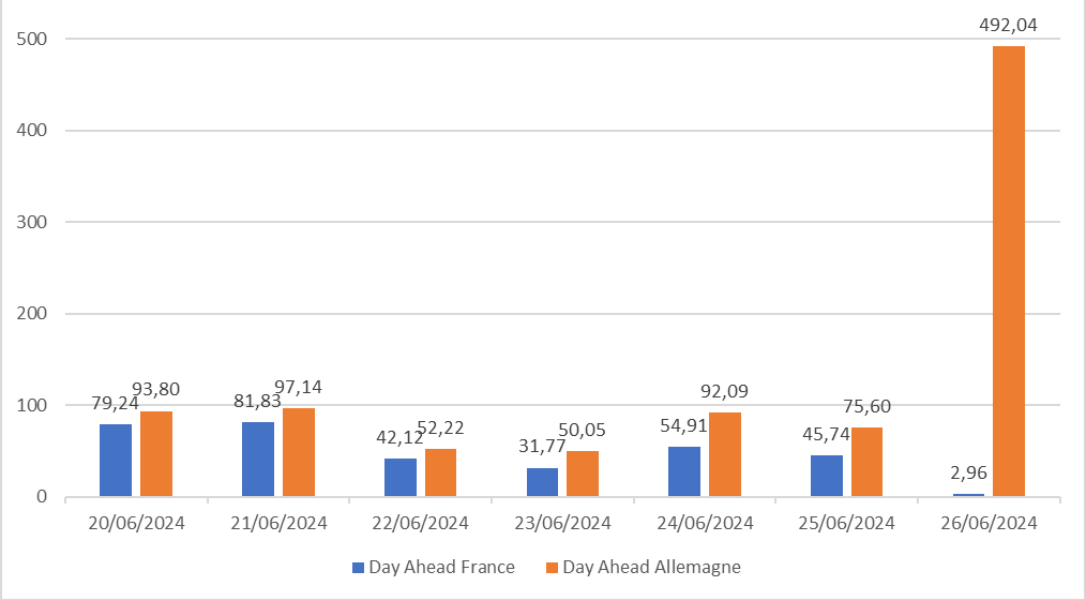
Un autre élément clé pour assurer la résilience des organisations de marché comme les bourses de l'électricité réside dans la sécurité informatique. L'énorme volumétrie des opérations, les flux d'information avec les différents acteurs de marché, les interactions avec les gestionnaires de réseau, les calculs pour définir les *clearing price* et les appels de marges et nombreuses autres fonctions nécessitent le déploiement de services informatiques performants et solides. Malgré les investissements effectués par les organisations de marché, des incidents sont régulièrement répertoriés, comme dans le cas du *market-decoupling* entre la France et l'Allemagne en juin 2024.

Encadré 8 – Focus sur l'incident de marché sur Epex Spot (juin 2024)

Le 25 juin 2024, la bourse EPEX SPOT a été confrontée à un incident technique qui a conduit à la fixation de prix Day-Ahead particulièrement hauts en Allemagne et bas en France pour la journée du 26 juin 2024. À la suite du déploiement d'une mise à niveau de fonctionnalité, sur le système de négociation d'enchères EPEX ETS, un problème technique s'est produit, entrainant un découplage des marchés EPEX SPOT.

L'impact a été très marqué sur les marchés français et allemand. Dans des conditions normales les prix allemands auraient été légèrement supérieurs aux prix français et la France aurait exporté de l'électricité vers l'Allemagne. En l'absence d'interconnexion disponible, le prix français pour la journée du 26 juin été fixé à 2,96€/MWh en moyenne sur la journée, alors que le prix allemand a été fixé à 492,04€/MWh, traduisant respectivement une abondance de production côté français et un équilibre offre/demande très tendu côté allemand.

Graphique 2 – Marchés Day-Ahead (J-1) français et allemands lors de l'incident Epex Spot de juin 2024



Source : Epex Power Spot, Day Ahead France-Allemagne.

La sécurité informatique est un élément fondamental pour assurer la continuité des opérations des marchés et représente donc une priorité pour les organisations de marché. Face aux risques d'incidents involontaires et d'actions malveillantes ayant des objectifs financiers ou politiques, les bourses et autres opérateurs multiplient les protections et les solutions de *back-up*.

Résilience en cas d'événements extrêmes

La question qui se pose est la suivante : comment fonctionneront les marchés en cas d'événements extrêmes comme des catastrophes naturelles ou des actes de sabotage qui impacteraient la disponibilité des réseaux de transport d'électricité (ou des unités de production) ? Quelles réactions, par exemple, en cas d'un sabotage provoquant la destruction d'une interconnexion entre 2 pays, ou l'arrêt d'une grande centrale de production ou encore l'impossibilité à approvisionner une région entière ?

D'un point de vue théorique, la conséquence de ces événements extrêmes sera la disparition d'un certain nombre d'ordres d'achat ou de vente au sein des procédures de fixations des prix de marché, avec des impacts conséquents sur les prix. Si on prend en considération en particulier le cas des marchés Day-Ahead, les courbes d'offre et de demande seront modifiées

dans le cadre des enchères quotidiennes tenues par les bourses d'électricité. Ainsi les prix qui sortiront de ces processus d'enchères vont refléter la réalité des indisponibilités physiques.

Les règles de fonctionnement des diverses bourses européennes prennent en compte un prix maximal pour les enchères[37]. Dans le cas où il n'est pas possible de fixer un *clearing price* par le biais de l'enchère - dans la situation où la totalité de la demande d'électricité ne peut être satisfaite par l'offre - les règles prévoient (a) le déclenchement de la *No Auction procedure* et la mise en place d'un *Pricing Committee* ad hoc qui établira un *clearing price* et (b) une proratisation de la demande. La proratisation de la demande signifie que le gestionnaire de réseau national aura ensuite la responsabilité de gérer les black-out qui seront nécessaires sur son réseau.

3. Anticiper le black-out : résilience des institutions et des populations, résilience militaire

La résilience du réseau de transport d'électricité européen en cas d'incident est globalement bonne et n'a cessé de s'améliorer depuis la reconstruction post conflit des années 1950. L'exemple ukrainien (cf. Partie 3) montre par ailleurs que même dans une situation de conflit de haute intensité, il est très difficile de mettre à bas l'ensemble de l'infrastructure de transport d'électricité d'un État de la plaque européenne.

Cependant, si l'effondrement prolongé d'une large partie du réseau de transport d'électricité européen est un risque faible, les black-out prolongés à des échelles locales redeviennent un risque avéré. C'est notamment le cas dans un contexte d'accroissement des événements climatiques extrêmes sur le sol européen. Ainsi la tempête Ciaran de 2023 en France a privé d'électricité un million de foyers pendant plus de 5h en décembre, pour certains pendant 15 jours, avec un coût d'indemnisation estimé pour Enedis à 130 millions d'euros. Les inondations de juillet 2021 en Allemagne ont quant à elles privé d'électricité pendant plusieurs jours autour de 200 000 foyers.

Cette résurgence des coupures d'électricités localisées s'accompagne d'une plus grande vulnérabilité des populations. Dans un contexte où l'électrification du chauffage (aujourd'hui 15% du chauffage résidentiel) est en croissance, une large part des ménages français et européens n'anticipe pas ou peu une potentielle rupture d'approvisionnement en électricité. Interrogés en 2022, les équipes de RTE, le gestionnaire du réseau de transport d'électricité français, indiquaient que leur marge de manœuvre temporelle pour le rétablissement du

[37] Le plafond, actuellement fixé à 4000 €/MWh, découle du règlement *Harmonised Maximum and Minimum Clearing Prices (HMMCP) Methodology in accordance with Article 41(1) of Commission Regulation (EU) 2015/1222 of 24th July 2015 (CACM Regulation*).

courant s'était significativement réduite : « Avant les gens commençaient à s'inquiéter quand les châteaux d'eau étaient vides parce que les stations de pompage ne fonctionnaient plus, on avait quelques jours devant nous, aujourd'hui c'est la panique au bout de quelques heures, quand les téléphones portables n'ont plus de batterie » (RTE, Entretien, 2022). La préparation et la résilience de la population à des ruptures d'approvisionnement en électricité fait partie d'une culture du risque qui existe dans d'autres parties du monde où les aléas environnementaux le justifient. C'est le cas dans certains États des États-Unis par exemple en cas d'incendies ou d'ouragans[38], ou en Norvège en cas de crises ou d'événements climatiques extrêmes. Ces Etats proposent alors à leur population des éléments de bonnes pratiques (gestion de l'eau, canaux d'accès à des informations fiables) et un kit d'outils et de consommables essentiels à conserver chez soi (lampe torche, kit de premiers secours, radio à piles). Cette culture du risque pourrait être développée en France et en Europe pour renforcer la résilience des populations.

Une question similaire se pose pour les armées. Si leur approvisionnement en énergie fait l'objet d'une planification logistique en opération, sur le territoire national la plupart des bases et emprises militaires dépendent du réseau d'électricité national. Certaines de ces emprises n'ont pas de point d'injection unique et partagent leur approvisionnement avec d'autres emprises civiles ce qui les rend difficilement identifiables pour le gestionnaire de réseau en cas de mise en œuvre de coupures d'urgence. Cela rend d'autant plus important la conduite de tests réguliers sur les générateurs de secours et sur les stocks de carburant associés. Aux États-Unis où les bases militaires doivent développer une résilience électrique, certaines ont mis en place des systèmes de *smart grids* activables en cas d'attaque sur le réseau national ou d'événement climatique extrême. Elles permettent aux emprises de s'isoler du reste du réseau pour fonctionner en autonomie avec de la production renouvelable locale et des réserves pendant des durées allant de quelques jours à plusieurs semaines[39].

[38] FEMA, Proper Emergency Kit Essential to Hurricane Preparedness, 2018 ; Norwegian directorate for civil protection, Advice on emergency preparedness
[39] Quil Lawrence, « The military is turning to microgrids to fight global threats — and global warming », *NPR*, 2 octobre 2023

CAS D'ÉTUDE : LE SYSTÈME ÉLECTRIQUE, ENJEU FONDAMENTAL DU CONFLIT RUSSO-UKRAINIEN

Depuis 2017, l'ENTSO-E et le gestionnaire du réseau de transport d'électricité ukrainien, Ukrenergo préparent la synchronisation de l'Ukraine avec la plaque électrique européenne. Le 24 février 2022, dans ce contexte du processus de synchronisation du réseau électrique ukrainien avec le réseau européen, le réseau ukrainien a été découplé des réseaux russe et biélorusse. Ce découplage était supposé n'être qu'un test de trois jours mais quatre heures après son commencement, la Russie a débuté son invasion[40]. Ce découplage marque alors le début d'une profonde et rapide transformation du système électrique hérité de l'époque soviétique qui s'opère actuellement sous les bombardements et en fonction des dégâts causés par ceux-ci[41].

Dès les premières semaines de l'invasion, l'armée russe a pris le contrôle de la centrale nucléaire de Zaporijjia. À partir de septembre 2022, cette centrale, la plus grande d'Europe (6 GW), a cessé d'approvisionner le réseau ukrainien. Les bombardements du système électrique ont commencé un mois plus tard. Une nouvelle vague de frappes au printemps 2024 a laissé le système électrique ukrainien exsangue.

Le système électrique ukrainien est un enjeu fondamental du conflit. Sur un plan stratégique, il conditionne la capacité à tenir de la population ukrainienne et le fonctionnement de l'industrie du pays. Au niveau tactique, la mise hors service des infrastructures électriques permet des effets de brouillard de guerre

1. Trois vagues de frappes successives et une évolution des cibles

Les attaques sur le réseau électrique ont débuté le 10 octobre 2022. En huit jours, 30% des centrales électriques du pays ont été détruites ainsi que de nombreuses lignes de transmission et postes électriques. L'Ukraine a cessé d'exporter de l'électricité vers l'UE et quatre millions de personnes ont subi des ruptures d'approvisionnements à la suite de cette première série de frappes[42]. En novembre 2022, les frappes sur le réseau ukrainien ont causé une rupture de l'approvisionnement en électricité sur près de la moitié du territoire de la Moldavie[43].

En dépit de la persistance des frappes, la situation du système électrique ukrainien a commencé à se stabiliser en février 2023 grâce aux réparations opérées. À la fin de cette première vague, en avril 2023, l'armée russe aurait, selon le Centre de recherche sur

[40] Paul Adams, « Ukraine War: On the Front Line with Engineers Working to Fix Stricken Power Grid », *BBC News*, 3 février 2023.
[41] La synchronisation du réseau ukrainien avec le réseau européen est effective depuis le 16 mars 2022.
[42] Santora, Marc, « Russia Says It's Suspending Participation in Grain Deal With Ukraine », *The New York Times*, 29 October 2022.
[43] « Moldova: Over half of country without electricity Nov. 23 », *Crisis24*, 23 novembre 2022.

l'industrie énergétique (EIRC) de Kiev, lancé plus de 1400 missiles et drones contre les infrastructures civiles de 17 oblasts[44] ukrainiens, touchant (sans forcément détruire complétement) la totalité des capacités de production thermiques et hydroélectriques[45].

Le 21 septembre 2023 marque le début de la seconde vague d'attaques russes contre le réseau électrique ukrainien. Lancée juste avant l'hiver, elle a duré environ trois mois et a été politiquement interprétée par le gouvernement ukrainien comme une tentative de faire plier la population civile en durcissant encore ses conditions de vie.

À partir du printemps 2024, l'armée russe a fait évoluer sa stratégie en comparaison aux frappes hivernales de 2022 et 2023. Les deux premières vagues de frappes visaient l'ensemble du système électrique en détruisant notamment beaucoup de postes électriques de distribution et de lignes de transport. Lors de la vague de frappes du printemps 2024, l'armée russe a davantage concentré ses tirs, de façon à saturer les défenses antiaériennes des capacités de production.

Encadré 9 – Le succès des frappes russes semble reposer sur un travail de renseignement ayant trait au dimensionnement de la défense aérienne ukrainienne[46].

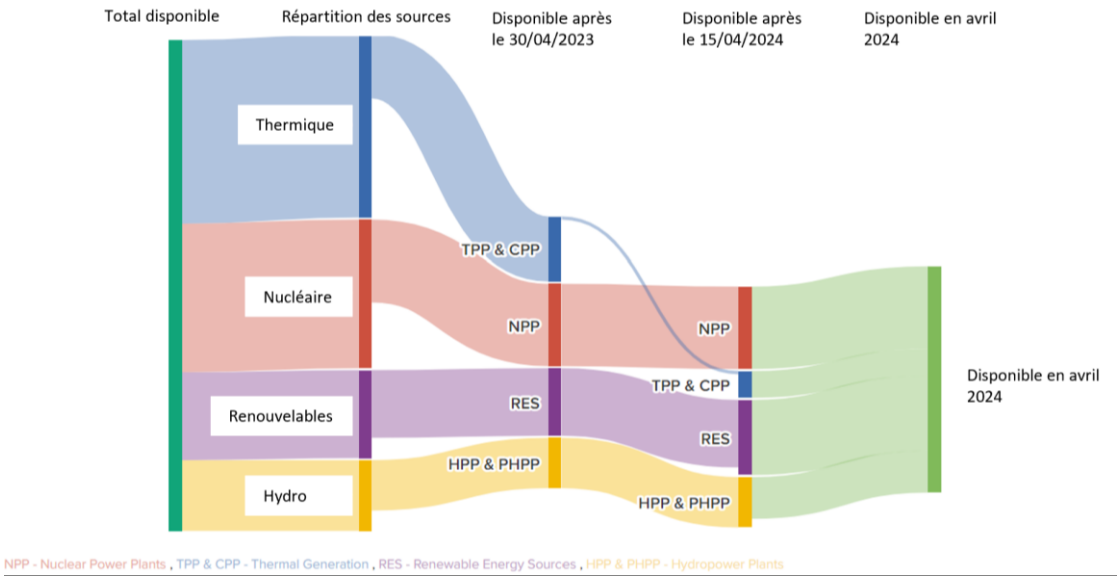
Le 11 avril 2024, la centrale thermique de Trypilska, essentielle à l'approvisionnement de la région de Kiev, a été détruite. Ce cas a été mis en avant par les autorités ukrainiennes pour illustrer le fait que ces destructions aux conséquences majeures sont les conséquences de l'insuffisance des capacités de défense aérienne. En réaction, le président Zelensky a déclaré : « onze missiles ont été lancés en direction de la centrale thermique de Trypilska [...]. Nous avons réussi à intercepter les sept premiers, mais les quatre autres ont frappé Trypilska. Pourquoi? Parce qu'il ne restait plus aucun missile. Nous avons épuisé tous les missiles qui défendaient Trypilska. » [47].

[44] Yale School of Public Health's Humanitarian Research Lab, *Remote assessment of bombardment of Ukraine's power generation and transmission infrastructure, 1 October 2022 to 30 April 2023 - a Conflict Observatory report* (New Haven: Humanitarian Research Lab at Yale School of Public Health and Ukraine Digital Verification Lab, 2024).
[45] Energy Charter, *Cooperation for Restoring the Ukrainian Energy, Infrastructure project*
Task Force, Ukrainian energy sector evaluation and damage assessment – VIII (as of March 24, 2023), (Brussels : Energy Charter Secretariat, 2022).
[46] Samya Kullab, « Russia renews big attacks on Ukrainian power grid using better intelligence and new tactics », *APNews*, 5 avril 2024.
[47] « 'Zero Missiles Left' - Zelensky Says Ukraine's Air Defence Resources Depleted », *KyivPost*, 16 avril 2024.

Les capacités de production demandent plus de temps et d'argent pour être réparées que les sous stations ou les ligne de transport. En se concentrant sur la destruction des capacités de production pilotables (thermiques et hydrauliques), la Russie porte atteinte à la flexibilité du réseau ukrainien, c'est-à-dire à sa capacité d'adaptation. À la destruction des capacités de production thermiques et hydroélectriques s'ajoute l'occupation de la centrale nucléaire de Zaporijia (la plus grande d'Europe) par l'armée russe depuis le début du conflit, ce qui contribue à diminuer grandement les capacités pilotables dont dispose le réseau ukrainien[48;49].

En avril 2024 les dégâts occasionnés sur le système électrique depuis le début du conflit s'élevaient à 11 milliards de dollars selon le ministre délégué à l'énergie ukrainien Mykola Kolisnyk[50]. Entre fin mars et fin juin 2024, entre 80 et 90 % des capacités de production thermique et plus de 50% des capacités de production hydrauliques auraient été détruites[51]. Au cours du printemps 2024, l'Ukraine aurait perdu 9GW de capacités de production[52].

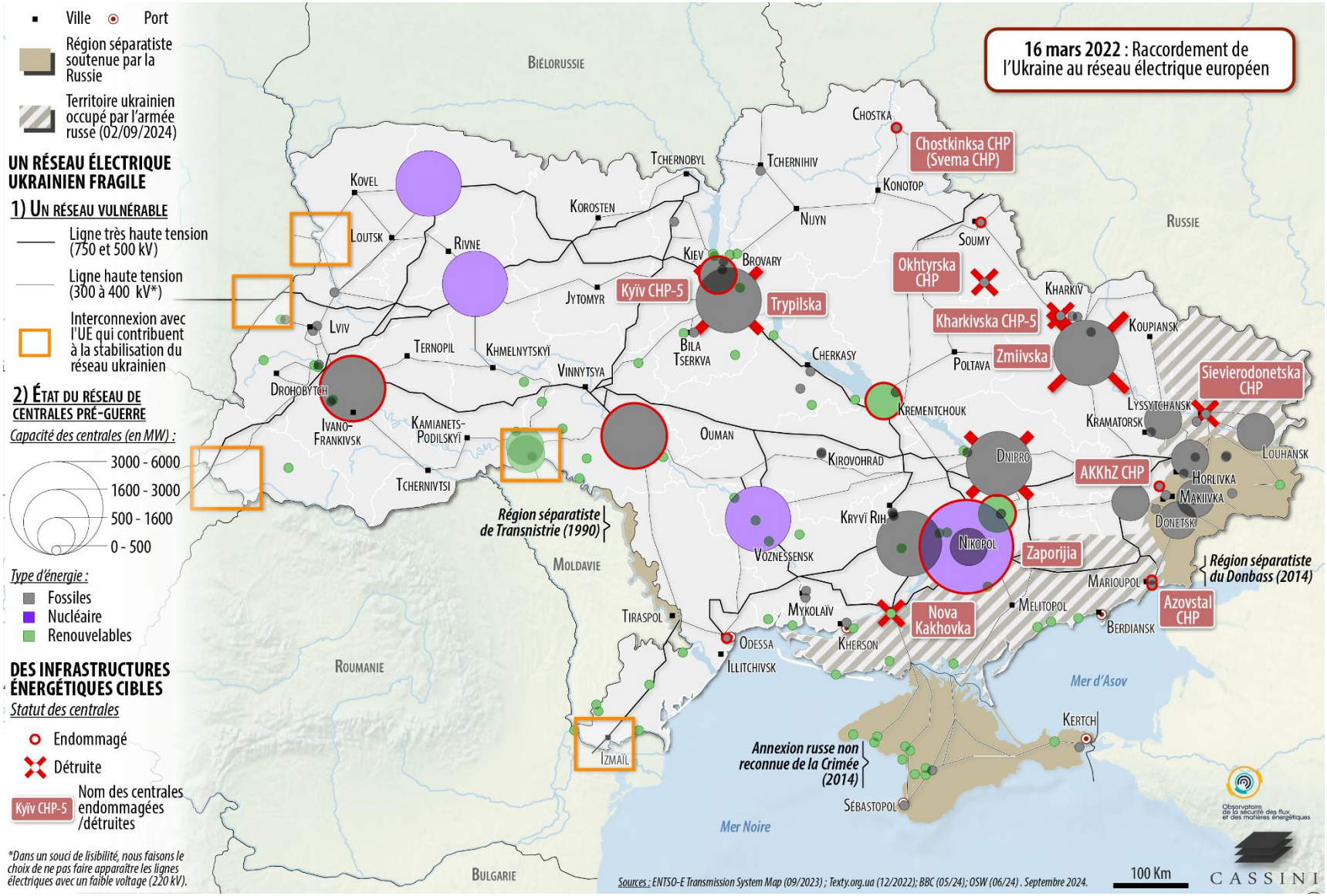
Graphique 3 – Disponibilité de la production d'énergie domestique en Ukraine 2022-2024



Source : Atlantic Council 2024[53]

[48] Environ 10 GW de capacité installée restent dans les territoires sous contrôle temporaire des forces russes et ne sont pas livrés au réseau, y compris les 6 GW de la centrale nucléaire de Zaporijia.
[49] Clara Marchaud, « Russia aims to destroy Ukraine's energy generation capacity », *Euractiv*, 19 avril 2024.
[50] Kateryna Pryshchepa, « "More air defence systems is the most effective means of supporting our power system" Interview with the Deputy Minister of Energy of Ukraine Mykola Kolisnyk », *New Eastern Europe*, 15 avril 2024.
[51] Sławomir Matuszak, « Russia's new large-scale attacks on Ukraine's energy infrastructure: losses and challenges », *Center for Eastern Studies* (2024).
[52] John E. Herbst et al., « Reconstructing Ukraine at War: The Journey to Prosperity Starts Now », Rapport de *Atlantic Council*, 2024.
[53] John E. Herbst et al., « Reconstructing Ukraine at War: The Journey to Prosperity Starts Now », Rapport de Atlantic Council, 2024.

Carte 7 – Le réseau électrique ukrainien à l'épreuve de la guerre



Le 26 août 2024, l'armée russe a lancé sa plus grande attaque de drones et missiles contre les infrastructures ukrainiennes depuis le début de l'invasion[54]. Alors que les frappes du printemps 2024 ciblaient principalement les capacités de production, celles du 26 août ont à nouveau visé des postes électriques. Plus particulièrement ceux des oblasts de Kiev, Vinnytsia, Zhytomyr, Khmelnytskyi, Dnipropetrovsk, Poltava, Mykolaiv, Kirovohrad et Odesa d'après un communiqué du ministère russe de la Défense[55].

En réaction à l'amélioration de la protection de ce genre d'infrastructures par les acteurs ukrainiens, l'armée russe a utilisé pour la première fois des missiles contre des postes électriques alors que lors des précédentes vagues elle s'était contentée de drones, réservant les missiles plus coûteux pour atteindre les capacités de production[56]. L'attaque a toutefois eu un impact sur les capacités de production ukrainiennes. En effet, les frappes ont entrainé la mise à l'arrêt de plusieurs réacteurs nucléaires[57].

Ainsi, après avoir détruit une grande partie des capacités de production thermiques et hydroélectriques, l'armée russe continuerait de s'attaquer aux capacités de production pilotables subsistantes sans pour autant prendre le risque de viser directement des infrastructures nucléaires.

2. Un mode opératoire qui combine frappes cinétiques et cyberattaques

En avril 2022, une cyberattaque ciblant les postes électriques d'une des principales entreprises énergétiques du pays a été déjouée[58], notamment grâce à l'appui de Microsoft et de la société de cybersécurité Eset. Si elle avait réussi, cette cyberattaque aurait pu impacter l'approvisionnement de deux millions de personnes. Les autorités ukrainiennes ont désigné le groupe de hackers lié au GRU, Sandworm, comme responsable. Sandworm aurait utilisé une nouvelle version du logiciel malveillant Industroyer qui, en 2016, avait déjà frappé des postes électriques entrainant des coupures d'électricité à Kiev. En 2015, Sandworm avait été identifié comme responsable de ce qui est considéré comme une des premières cyberattaques réussies à l'encontre d'un réseau électrique (cf. Encadré n°2).

Le 10 octobre 2022, concomitamment au début de la première vague de frappes contre le réseau électrique, une cyberattaque attribuée à Sandworm a frappé des infrastructures

[54] 236 missiles et drones se sont abattus sur 15 des 24 oblasts ukrainiens.
[55] Dinara Khalilova, Andrea Januta, Kateryna Denisova A near-death feeling:' Largest-yet Russian attack on Ukraine's energy infrastructure brings back widespread power outages, *The Kyiv Independent*, 26 aout 2024.
[56] Daria Svitlyk, « Russia struck energy substations with cluster munition missiles for first time, PM Shmyhal says », *The Kyiv Independent*, 23 Septembre 2024.
[57] Pavel Polityuk, Olena Harmash, « Russian attacks on power sector pose risk to nuclear facilities, Ukraine says », *Reuters*, 29 aout 2024.
[58] Joe Tidy, « Ukrainian power grid 'lucky' to withstand Russian cyber-attack », *BBC*, 12 avril 2022.

électriques avec succès coupant ainsi l'approvisionnement dans une zone qui n'a pas été identifiée. Selon le chef du département de cybersécurité du SBU, Illia Vitiuk, cette cyberattaque a probablement été menée pour maximiser l'impact des frappes de drones et missiles[59]. L'intrusion des hackers dans le système de la sous-station touchée aurait été opérée en juin 2022[60]. Cette cyberattaque serait un premier exemple de coordination d'attaques cyber et cinétiques.

Au printemps 2024, de nombreuses cyberattaques contre des infrastructures énergétiques ont été constatée. La coordination des attaques cyber et cinétiques semble désormais un mode opératoire établie. Un certain nombre de ces attaques cyber viserait spécifiquement à collecter du renseignement permettant d'évaluer les dommages causés par les frappes physiques de missiles[61]. Cela pourrait, entre autres, expliquer la précision croissante des frappes de drones et missiles sur les infrastructures électriques.

3. Le réseau électrique, objectif de guerre dans la doctrine militaire russe

Les responsables russes ont fait plusieurs déclarations publiques à travers lesquelles ils admettent que la Russie cible le système énergétique ukrainien et ils fournissent des arguments contradictoires pour justifier ces attaques. Les justifications données par les responsables russe relativement au ciblage du système énergétique relèvent de trois catégories : 1) la réalisation des objectifs militaires de la Russie ; 2) les représailles aux actions présumées de l'Ukraine[62] ; 3) l'infliction intentionnelle de dommages sur les civils dans le but d'obliger l'Ukraine à se soumettre aux exigences russes dans le cadre des négociations[63].

Les deux dernières catégories de justifications induisent potentiellement le viol du droit international humanitaire[64]. Le 5 mars 2024, la Cour pénale internationale (CPI) a inculpé le général Sergueï Kobylash, commandant des forces aérospatiales russes, et l'amiral Viktor Sokolov, commandant de la flotte de la mer Noire, pour crimes de guerre et crimes contre

[59] James Pearson, « Russian spies behind cyber attack on Ukraine power grid in 2022 – researchers », *Reuters*, 9 décembre 2023.
[60] Christioan Vasquez, Aj Vicens, « Russian hackers disrupted Ukrainian electrical grid last year », *Cyberscoop*, 9 novembre 2023.
[61] Ukraine's computer emergency response team (CERT-UA), « UAC-0133 (Sandworm) planifie le cyber-sabotage de près de 20 infrastructures critiques en Ukraine », En ligne, 19 avril 2024.
[62] Vladimir Poutine a justifié les premières frappes du 10 octobre 2022 en affirmant qu'elles étaient une réponse à l'attaque du pont de Crimée survenue deux jours plus tôt.
[63] Le vice-président du Conseil de sécurité de la Russie, Dmitriy Medvedev, a écrit sur Telegram en octobre 2022 que pour que l'Ukraine puisse stabiliser son approvisionnement énergétique, il était « nécessaire de reconnaître les demandes légitimes de la Russie dans le contexte de l'opération militaire spéciale et de ses résultats » et a laissé entendre que, lorsque l'Ukraine reconnaîtra les demandes de la Russie, « alors les lumières fonctionneront à nouveau ». https://t.me/medvedev_telegram/200
[64] Yale School of Public Health's Humanitarian Research Lab, *Remote assessment of bombardment of Ukraine's power generation and transmission infrastructure, 1 October 2022 to 30 April 2023 - a Conflict Observatory report* (New Haven: Humanitarian Research Lab at Yale School of Public Health and Ukraine Digital Verification Lab, 2024).

l'humanité perpétrés par des attaques contre des biens civils, causant incidemment des dommages excessifs à des civils ou à des biens civils, lors des attaques contre l'infrastructure électrique ukrainienne d'octobre 2022 à mars 2023[65]. Le 25 juin 2024, la CPI a inculpé l'ancien ministre de la Défense russe Sergei Shoigu et le chef d'état-major général des armées Valery Gerasimov pour les mêmes chefs d'accusation.

D'après le ministère de la Défense du Royaume-Uni, avec ce ciblage du réseau électrique ukrainien, la Russie mettrait en œuvre pour la première fois le concept d'« opération stratégique pour la destruction de cibles critiques importantes » (Strategic Operation for the Destruction of Critically Important Targets) dans le cadre des évolutions récentes de la doctrine militaire russe[66].

Les frappes russes portent gravement atteinte aux conditions de vie des civils ukrainiens. La destruction du système électrique produit un effet domino qui donne lieu à des coupures d'eau, de chauffage, de réseaux mobile et internet etc… Cette situation pousse les civils à la migration. Les attaques du printemps 2024 ont conduit la Banque Nationale d'Ukraine à réévaluer à la hausse ses prévisions concernant les départs de citoyens ukrainiens de leur pays en 2024 et 2025[67]. Outre les difficultés liées à l'absence de services basiques, les migrations sont également dues à la chute de la demande sur le marché du travail engendrée par le ralentissement de l'activité économique que cause les limitations de l'approvisionnement énergétique

Les limitations de l'approvisionnement énergétique ont d'autant plus d'impact sur l'économie ukrainienne que celle-ci repose en partie sur des secteurs industriels très énergivores comme la métallurgie (10% du PIB et 30% des recettes d'exportation)[68] . De plus, le ralentissement de la production industrielle impacte notamment l'industrie de défense ukrainienne justement au moment où celle-ci cherche à augmenter sa production.

4. Comment renforcer la résilience du système électrique ukrainien ?

Avec 59 gigawatts de puissance installée, l'Ukraine comptait avant 2022 parmi les plus grands producteurs d'énergie en Europe. Le pays lui-même avait besoin de 22 gigawatts. L'Ukraine disposait donc d'importantes réserves de capacité. Le pic d'appel de puissance (pic de demande) en Ukraine devrait atteindre 18 GW au cours de l'hiver 2024-2025. À cette période,

[65] Cour pénale internationale, « Situation en Ukraine : les juges de la CPI délivrent des mandats d'arrêt contre Sergei Ivanovich Kobylash et Viktor Nikolayevich Sokolov », Communiqué de presse, Bruxelles, 5 mars 2024.
[66] UK Ministry of Defence, « Intelligence update on Ukraine », compte Twitter/X, 1er décembre 2022.
[67] NBU expects outflow of 700,000 Ukrainians abroad in 2024-2025, *Interfax Ukraine*, 2 août 2024.
[68] Guillaume Ptak, « Pilier de l'économie ukrainienne, la métallurgie pâtit de la guerre », *Les Echos*, 19 décembre 2023.

les capacités disponibles des grandes centrales électriques conventionnelles ne devraient être que de 10,5 GW. En tenant compte de la contribution des énergies renouvelables et de l'électricité importée, le déficit pourrait être réduit à 5,8 GW[69]. Cette partie présente les options envisagées pour gérer cette carence et renforcer la résilience du réseau ukrainien.

Limitation de la consommation

De façon à préserver l'approvisionnement des consommateurs critiques tels que les hôpitaux où les installations militaires, les autorités ukrainiennes ont mis en place des coupures de courant tournantes concernant les foyers et les industries de l'ensemble du pays. À l'été 2024, des coupures de courant de dix heures étaient rapportées[70]. Cette situation pourrait fortement s'aggraver à l'hiver 2024, lorsque la demande augmentera, si les efforts consentis pour réparer les capacités de production et en construire de nouvelles ne sont pas suffisant. Dans les zones les plus impactées, des « centres de résilience » peuvent être mis en place pour accueillir un certain nombre de civils et leur fournir un accès à l'électricité ainsi qu'à d'autres services de base[71]. Ces coupures tournantes sont utilisées en cas de rupture d'approvisionnement majeures par les gestionnaires de réseau (comme au Venezuela lors des black-out de 2022 après l'arrêt de la plus grande centrale hydroélectrique du pays). Elles permettent d'assurer un contrôle de la demande et de conserver la main sur la stabilité du réseau.

Renforcement de la défense antiaérienne

Il s'agit de la demande principale des acteurs ukrainiens qui ne pourront réparer et reconstruire durablement le système électrique tant que le ciel n'est pas sécurisé. Dès les premiers mois de l'invasion, la Slovaquie a fourni un système russe S300[72]. En octobre 2022, l'Allemagne a livré un premier exemplaire des systèmes Iris-T qu'elle fabrique[73]. Cependant, le principal système demandé par les autorités ukrainiennes est le système Patriots de fabrication américaine. À l'été 2024, les Ukrainiens estimaient avoir besoin de sept systèmes Patriots supplémentaires pour être en mesure de protéger leurs infrastructures[74]. Le porte-parole du Conseil de sécurité nationale des États-Unis, John Kirby, a déclaré fin juin 2024 que Washington placerait l'Ukraine en tête de la file d'attente pour les livraisons de Patriots,

[69] Susanne Nies et Oleh Savytskyi, *Six options to boost power transfers from Continental Europe to Ukraine, for the next two winters*, Report Green Deal Ukraina (Berlin : Helmholtz Centrum Berlin, 2024).
[70] *Ibid.*
[71] Yogita Limaye, « Ukraine War: Defying Russian Onslaught in City "at the End of the World" », *BBC*, 4 janvier 2023.
[72] David Vergun, « Slovakia to Supply S-300 Air Defense System to Ukraine », *US Department of Defense*, 8 avril 2022.
[73] Dan Sabbagh et Patrick Wintour, « Ukraine Says 30% of Its Power Plants Destroyed in Last Eight Days », *The Guardian*, 18 octobre 2022.
[74] Jean Mackenzie, « Ukraine Extends Blackouts as Russian Bombings Continue », *BBC News*, 12 juin 2024.

devant les autres pays qui les ont commandées. Les États-Unis n'avaient alors livré que deux systèmes Patriots[75], tandis que l'Allemagne en avait livré trois (ce qui représente un quart des capacités du pays)[76]. Les Pays-Bas et la Roumanie ont promis d'en livrer un chacun[77]. À la fin aout 2024, le ministre des Affaires étrangères ukrainien a appelé à une accélération de la livraison des systèmes de défense antiaériens. Les obstacles pour ces livraisons viennent principalement du coût des équipements et de la réticence des partenaires à affaiblir leurs propres capacités.

Outre la défense anti aérienne, les infrastructures doivent également être protégée par un renforcement de la cybersécurité et des équipements de protection construits autour d'elles.

Développement de capacités de production décentralisées

Développer des capacités de production décentralisées permettrait de reconstruire le système électrique ukrainien en le rendant moins vulnérable aux frappes russes. En effet, une multitude d'unités de production dispersées géographiquement serait bien plus difficile à cibler physiquement que quelques grosses centrales thermiques, cela implique en revanche un important effort de cybersécurité.

L'Ukraine possède un potentiel important pour la production d'énergies renouvelables (éolien, solaire, hydroélectrique et géothermique). Il s'agirait donc de construire de petites unités de production d'électricités renouvelables en combinaison avec des capacités de stockages (telles que des batteries) mais aussi de petites unités de production au gaz afin de préserver la pilotabilité du système. Les centrales à gaz ont l'avantage de pouvoir produire à la fois de l'électricité et de la chaleur, ce qui pourrait contribuer à compenser la destruction des grandes centrales de cogénération ukrainiennes. La construction de petites centrales de cogénération au gaz sur de nouveaux sites pourrait ajouter 600 MW supplémentaires dans un délai d'un an et demi selon le Think Tank Green Deal Ukraïna [78]. En plus des petites centrales à gaz, la stratégie de décentralisation de la production comprend la mise en place de générateurs. Des capacités de production pourraient être installées sur les infrastructures critiques (telles que les hôpitaux) de façon à ce qu'elles soient autosuffisantes. Il reste à savoir

[75] US Department of Defense, « Fact Sheet on U.S. Security Assistance to Ukraine », 9 août 2024.
[76] Chancellerie d'Allemagne, « The arms and military equipment Germany is sending to Ukraine», 19 septembre 2024, https://www.bundesregierung.de/breg-en/service/military-support-ukraine-2054992
[77] Nikolov Boyko, « Ukraine Gets 3 Patriot Systems from Netherlands, Romania, Germany », *Bulgarianmilitary.Com* (blog), 28 juin 2024.
[78] Susanne Nies et Oleh Savytskyi, *Six options to boost power transfers from Continental Europe to Ukraine, for the next two winters*, Report Green Deal Ukraina (Berlin : Helmholtz Centrum Berlin, 2024).

en combien de temps l'Ukraine pourrait mettre en œuvre un système de production décentralisé[79].

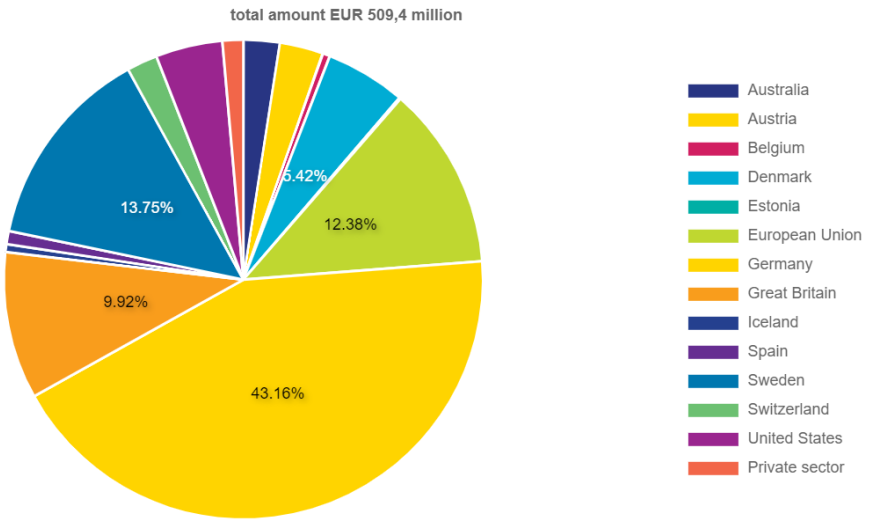
Le développement de petites unités de production nécessite d'importants investissements privés qui comportent un risque très important au vu du contexte sécuritaire en Ukraine. Entrer sur le marché ukrainien maintenant, avant que la reconstruction ne prenne de l'ampleur, donnerait cependant aux entreprises concernées un avantage concurrentiel et les autorités ukrainiennes espèrent attirer les investisseurs privés en initiant des changements réglementaires, notamment en libéralisant les prix de l'électricité. Cette libéralisation peut renforcer l'attractivité économique du système électrique mais elle révèle un des principaux défis posés par le développement de capacités décentralisées : celui de maintenir un prix de l'électricité abordable pour les foyers et les consommateurs industriels. En effet, il est beaucoup moins coûteux de produire de l'électricité à grande échelle.

Faciliter l'acheminement de pièces de rechange ainsi que la construction sur place

Réparer et développer le système électrique ukrainien demande un approvisionnement conséquent de pièces de rechange. De façon à organiser et optimiser ce flux, le Ukraine Energy Support Fund a été créé à l'initiative du ministre de l'Énergie ukrainien, German Galushchenko, et de la Commissaire européenne à l'Énergie, Kadri Simson. Lorsqu'il faut restaurer des équipements endommagés par les bombardements, la partie ukrainienne collecte les informations sur les besoins et la Communauté de l'énergie gère les achats via le fond. Ces achats sont effectués grâce aux contributions d'acteurs étatiques en grande majorité.

[79] Sławomir Matuszak, « Russia's new large-scale attacks on Ukraine's energy infrastructure: losses and challenges », Center for Eastern Studies, Analyses, 17 avril 2024.

Graphique 4 – Contributions au Ukraine Energy Support Fund par pays



Source : Energy Community s.d.[80]

Outre la fourniture de pièces neuves, les partenaires de l'Ukraine peuvent également puiser dans les pièces des centrales électriques déclassées (centrales à charbon notamment) comme l'a proposé la Lituanie[81]. Cela est principalement valable pour les pays disposant de technologies soviétiques à l'instar de ce qui est en usage en Ukraine.

Les acteurs ukrainiens ont des besoins urgents en pièces de rechange alors que le marché mondial des équipements est tendu du fait de la forte demande engendrée par les stratégies de transition énergétique. Afin d'atténuer les goulets d'étranglement dans les chaines de valeur, des coentreprises pourraient être créées entre les fournisseurs extérieurs et des entreprises ukrainiennes afin d'augmenter les capacités de production de pièces et rapprocher géographiquement cette production des besoins.

Avec un approvisionnement optimal des pièces nécessaires à la réparation des centrales hydroélectriques et thermiques, Green Deal Ukraïna estime qu'une capacité de 1 GW pourrait être restaurée d'ici l'hiver 2025/26[82].

Agrandir les interconnexions reliant l'UE à l'Ukraine

Exportatrice d'électricité vers l'UE entre la synchronisation de son réseau avec celui de l'UE (16 mars 2022) et le début des frappes russes sur le réseau (10 octobre 2022), l'Ukraine est

[80] Energy Community, « Ukraine Energy support Fund », https://www.energy-community.org/Ukraine/Fund.html (page consultée le 24 juillet 2024)
[81] Dmytro Basmat, « Energy Minister: Lithuania offers to dismantle shuttered energy stations, provide Ukraine with spare parts », *The Kyiv Independent*, 19 avril 2024.
[82] Susanne Nies et Oleh Savytskyi, *Six options to boost power transfers from Continental Europe to Ukraine, for the next two winters*, Report Green Deal Ukraina (Berlin : Helmholtz Centrum Berlin, 2024).

aujourd'hui dépendante des importations depuis l'UE[83]. Les interconnexions reliant l'UE à l'Ukraine ne permettent actuellement que de transporter qu'1,7 GW/heure. Cette limite est régulièrement presque atteinte depuis mai 2024. En remédiant aux déficits actuels des systèmes hongrois, slovaque, polonais, roumain et ukrainien, les interconnexions reliant l'UE à l'Ukraine pourraient permettre de transporter 2 GW vers l'Ukraine à l'hiver 2024-2025 et 2,2 GW pour l'hiver 2025/2026. Outre l'amélioration des capacités existantes, de nouvelles lignes de transmission devraient être construites entre la Slovaquie et l'Ukraine d'une part et entre la Roumanie, la Moldavie et l'Ukraine d'autre part. Au-delà de ces solutions, le rapport du think tank Green Deal Ukraïna, intitulé « Six options to boost power transfers from Continental Europe to Ukraine, for the next two winters », explore d'autres solutions qui permettraient à l'Ukraine de recevoir plus d'électricité depuis le réseau de ses voisins.

CONCLUSION

Le réseau d'électricité européen a connu d'importantes évolutions sur les dernières décennies, qu'il s'agisse d'infrastructures, d'interconnexions, de changement des sources d'énergie dont il assure le transport ou d'ouverture au numérique pour assurer le pilotage de la production. Ces évolutions ont transformé sa vulnérabilité, qu'il s'agisse des effets d'attaques, cyber ou physique, ou de la croissance des événements climatiques extrêmes sur le sol européen, et ce alors que le réseau électrique est devenu aujourd'hui une infrastructure particulièrement critique pour les sociétés industrialisées. Ces évolutions si elles ne sont pas entièrement spécifiques à l'UE correspondent à l'historique de la construction du réseau dont les profils sont différents pour d'autres espaces.

Aux États-Unis, le gouvernement fédéral n'a pas cherché à intégrer les réseaux des différents États dans un système unifié et l'échelon fédéral gère principalement des interconnexions entre plusieurs systèmes aux caractéristiques et vulnérabilités distinctes. La Chine a inversement pris comme exemple le modèle d'intégration européen et cherche à construire un système relativement unifié à l'échelle nationale, appuyé sur le développement de technologies de transport sur grande distance avec notamment pour objectif d'intégrer à l'alimentation de la zone de production côtière de la production, notamment renouvelable, située dans l'intérieur des terres. D'autres modèles existent, comme celui actuellement débattu pour plusieurs États du continent africain, autour du concept d'un réseau non intégré constitué d'une pluralité de petits réseaux indépendants, permettant d'économiser le coût en

[83] Ces importations engendrent un surcoût comparé à ce qui aurait pu être produit localement.

ressources de grandes infrastructures de transport, dans un environnement particulièrement éprouvant pour les matériels.

Dans ce contexte d'évolution des vulnérabilités pour une architecture électrique européenne unique en son genre, les enseignements du ciblage du système électrique ukrainien et les moyens mis en œuvre pour assurer sa résilience sont riches pour les gestionnaires de réseaux de transport d'électricité européens. :

- Dès les prémices du conflit, après les attaques cyber menées sur le réseau électrique en 2016, puis en 2017-2018, l'Ukraine a travaillé à améliorer sa posture cyber, avec l'appui d'entreprises américaines comme Microsoft ou CISCO et en travaillant à la redondance et à la mobilité des centres de sécurité.
- Un important effort de formation et de sensibilisation des utilisateurs d'infrastructures IT a été et reste fourni par le gestionnaire du réseau de transport d'électricité ukrainien pour éviter les intrusions de type phishing dans ses infrastructures. Il s'avère payant au sens où si la partie russe multiplie les attaques simples (déni de service, phishing), les infections profondes du système électrique semblent avoir été évitées à ce stade.
- La redondance des infrastructures de pilotage de la production est aujourd'hui clé dans la résilience du système électrique ukrainien. Elle passe par le développement de systèmes mobiles de pilotage des flux (dont certains tiennent dans une camionnette), mais aussi de systèmes multiconnectés dont l'enjeu est aujourd'hui de les rendre utilisables y compris dans un contexte d'utilisation des systèmes de brouillage antimissiles utilisés par l'Ukraine pour défendre ses infrastructures électriques.
- Les interconnexions avec le reste du réseau européen sont vitales pour l'architecture électrique de l'Ukraine à qui elles apportent une profondeur et une inertie qui permettent de résister aux perturbations causées par les attaques russes. Ce constat vaut pour le reste du réseau européen en cas de perturbation majeure et ce quelle qu'en soit la cause.

L'Ukraine fonde ainsi sa résilience électrique sur un mélange entre, une grande flexibilité d'opération du réseau, le développement d'infrastructures mobiles très intensives en technologie et la conservation d'une capacité d'intervention manuelle extrêmement rustique par les équipes sur le terrain. Cet ensemble est appuyé par le soutien du réseau européen et des États de l'UE qui fournissent des pièces et infrastructures de rechange.

L'ANALYSE GÉOPOLITIQUE DES ENJEUX ÉNERGÉTIQUES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

L'Observatoire de la sécurité des flux et des matières énergétiques est coordonné par l'IRIS, en consortium avec Enerdata et Cassini, dans le cadre d'un contrat réalisé pour le compte de la Direction générale des relations internationales et de la stratégie (DGRIS) du ministère des Armées. Il est coordonné par Sami Ramdani, chercheur à l'IRIS, et rassemble une équipe d'une vingtaine de chercheurs et professionnels.

DGRIS

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Enerdata
intelligence + consulting

CASSINI

www.iris-france.org