Observatoire
de la sécurité des flux
et des matières énergétiques

SYNTHÈSE

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.

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 communication en dépendent. Les sociétés occidentales (en s'intéressant 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 XXI^{e} siècle des cibles physiques et sont largement concernés par des menaces cyber. Ils jouent 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.

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 Seconde Guerre mondiale, puis des éléments stratégiques de la reconstruction européenne après le conflit ainsi que pendant la guerre froide. 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 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, puis les campagnes de frappes russes sur les infrastructures électriques ukrainiennes depuis l'invasion du 24 février 2022, mais aussi les intrusions dans les réseaux de plusieurs États membres de l'OTAN, ont remis les réseaux de transport d'électricité au cœur des préoccupations de la résilience nationale.

Le contexte dans lequel s'inscrit la gestion de ces réseaux a également beaucoup évolué depuis le début des années 2000. Dans l'UE, l'intégration des réseaux, la transition énergétique et l'électrification des usages qu'elle entraine, ainsi que la numérisation et les effets du changement climatique, ont transformé la vulnérabilité de l'architecture de transport électrique européenne. Ces transformations interviennent dans un contexte d'interdépendance où les frontières de l'Europe électrique ne sont pas celles de l'Europe politique. 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 et cinq zones synchrones.

La sécurité des réseaux et du système électrique européen ne relève alors 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 évènement 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.

1. Vulnérabilité et protection des réseaux de transport d'électricité européens

La protection physique des réseaux redevient un enjeu

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, et les gestionnaires de réseau de transport d'électricité européens se perçoivent comme des infrastructures « normales », sans dimension stratégique particulière. 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.

Les aléas physiques auxquels sont soumis ces réseaux proviennent également de la croissance des évènements 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 pour gérer notamment les effets des ouragans et des grands incendies qui touchent désormais régulièrement la côte ouest des États-Unis. 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. Si l'ENTSO-E n'organise pas d'exercice de gestion de crise 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[1].

[1] 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.

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 »[2].

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. 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 : Agence de l'Union européenne pour la cybersécurité (ENISA)).

L'interdépendance croissante entre technologies de l'information et de la communication (TIC) et secteur électrique ajoute au caractère critique de ce dernier. Les systèmes de pilotage par la donnée en cours de construction dans la plupart des secteurs allant de l'internet des objets aux *smart cities*, dépendent d'un approvisionnement électrique continu. Une perturbation de cet approvisionnement aurait un impact 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 *smart grids* permet aussi un phénomène de résilience des réseaux.

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. Si les résultats de l'exercice sont positifs, l'enjeu pour les parties prenantes a été de coordonner rapidement leurs actions et leurs réponses notamment dans leur dimension transfrontalière.

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

[2] Future of our Grids, « Discussion and Conclusions of the High-Level Forum », 7 septembre 2023, Brussels. https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/events/2023/230907_SessionIII_Discussion and Conclusions_for publication.pdf

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.

Sécurité économique, gestion des investissements étrangers

La sécurité physique et cyber du réseau de transport d'électricité européen repose, 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-19 et des tensions grandissantes entre la Chine et l'UE, le solaire photovoltaïque continue de tirer les investissements chinois en UE.

Dans le cadre de son projet des nouvelles Routes de la soie 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, a multiplié les prises de participations dans les réseaux européens. Cela lui confère une visibilité sur la stratégie de développement des réseaux de transports d'électricité européens ainsi que sur leurs vulnérabilités.

2. Résilience des infrastructures, des marchés et des populations

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.

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. Dans le cas des réseaux de transport d'électricité, l'UE prend en compte le risque cyber à une échelle européenne avec les directives « Sécurité des réseaux et de l'information » (NIS), les exercices de l'ENISA et des codes de réseaux communs définis par l'ENTSO-E dont les normes cyber sont en cours de mise en œuvre. La sécurité des mécanismes de marché est également envisagée à une échelle européenne. La sécurité des flux est construite à une échelle infrarégionale, qui rassemble des groupes d'États voisins au sein de six coordinateurs régionaux de sécurité, 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 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. Comparativement, l'UE manque encore d'exercices de grande envergure menés à l'échelle européenne et comprenant plusieurs dimensions de sécurité.

Résilience des marchés européens

Des avantages économiques et une sécurité énergétique renforcée résultent de l'intégration des marchés européens de l'électricité qui permet des synergies croissantes, notamment dans un contexte de transition énergétique et de développement de la production renouvelable. 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. L'intégration des marchés implique cependant aussi qu'en cas d'incident les risques des effets de « cascade » et de propagation entre différentes zones augmentent.

Une large partie de la résilience des organisations de marché comme les bourses de l'électricité réside dans la sécurité informatique qui soutient le très important volume des opérations et des flux d'information entre acteurs du marché. 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. Face aux risques d'incidents involontaires et d'actions malveillantes, les bourses et autres opérateurs cherchent à multiplier les protections et les solutions de *back-up*.

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 montre par ailleurs que même dans une situation de conflit de haute intensité, il est 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 évènements climatiques extrêmes en Europe. 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 plus de 15 jours. 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. 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, ou en Norvège en cas de crises ou d'évènements climatiques extrêmes. Ces États 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.

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'évènement 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.

3. Cas d'étude : Le système électrique, enjeu fondamental du conflit russo-ukrainien

Le système électrique est un enjeu fondamental du conflit russo-ukrainien. Il conditionne la capacité à tenir de la population ukrainienne et le fonctionnement de l'industrie du pays.

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. Une seconde vague de frappes débute en septembre 2023. 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. Si les deux premières vagues de frappes visaient l'ensemble du système électrique en détruisant notamment postes électriques et de lignes de transport. Au printemps 2024, l'armée russe a davantage concentré ses tirs sur les capacités de production, de façon à saturer leurs défenses antiaériennes.

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 par l'armée russe depuis le début du conflit, ce qui contribue à diminuer grandement les capacités pilotables dont dispose le réseau ukrainien[3]. En avril 2024, les dégâts cumulés

[3] 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.
Clara Marchaud, « Russia aims to destroy Ukraine's energy generation capacity », *Euractiv*, 19 avril 2024.

sur le système électrique depuis le début du conflit atteignaient 11 milliards de dollars selon le ministre de l'Énergie ukrainien Mykola Kolisnyk[4].

En aout 2024, l'armée russe frappe de nouveau les infrastructures de transport et de distribution. Face à l'amélioration de leur protection par les acteurs ukrainiens, elle utilise 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. En atteignant, à travers le réseau, la capacité de pilotage de la production, ces frappes ont conduit à la mise à l'arrêt de plusieurs réacteurs nucléaires.

Le mode opératoire russe 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[5], 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 avait déjà été identifié en 2015 comme responsable de ce qui est considéré comme une des premières cyberattaques réussies à l'encontre d'un réseau électrique.

Le 10 octobre 2022, au début de la première vague de frappes contre le réseau électrique, une cyberattaque attribuée à Sandworm a frappé des infrastructures électriques avec succès coupant ainsi l'approvisionnement dans une zone qui n'a pas été identifiée. Selon le chef du département de cybersécurité du Service de sécurité d'Ukraine (SBU), Illia Vitiuk, cette cyberattaque a probablement été menée pour maximiser l'impact des frappes de drones et missiles[6]. L'intrusion des hackers dans le système de la sous-station touchée aurait été opérée en juin 2022[7]. 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

[4] Kateryna Pryshchepa, « More air defence systems is the most effective means of supporting our power system », entretien avec le vice-ministre ukrainien de l'énergie Mykola Kolisnyk, *New Eastern Europe*, 15 avril 2024.
[5] Joe Tidy, Ukrainian power grid 'lucky' to withstand Russian cyber-attack, *BBC*, 12 avril 2022. https://www.bbc.com/news/technology-61085480
[6] James Pearson, « Russian spies behind cyber attack on Ukraine power grid in 2022 – researchers », *Reuters*, 9 décembre 2023. https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/
[7] Christioan Vasquez, Aj Vicens , « Russian hackers disrupted Ukrainian electrical grid last year », *Cyberscoop*, 9 novembre 2023. https://cyberscoop.com/sandworm-russia-ukraine-grid/

physiques de missiles[8]. Cela pourrait, entre autres, expliquer la précision croissante des frappes de drones et missiles sur les infrastructures électriques.

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. D'après le ministère de la Défense du Royaume-Uni (Publication Twitter/X, 2022), avec ce ciblage du réseau électrique ukrainien, la Russie mettrait en œuvre pour la première fois son concept d'« opération stratégique pour la destruction de cibles critiques importantes ».

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). Le ralentissement de la production industrielle touche notamment l'industrie de défense ukrainienne.

Comment renforcer la résilience du système électrique ukrainien ?

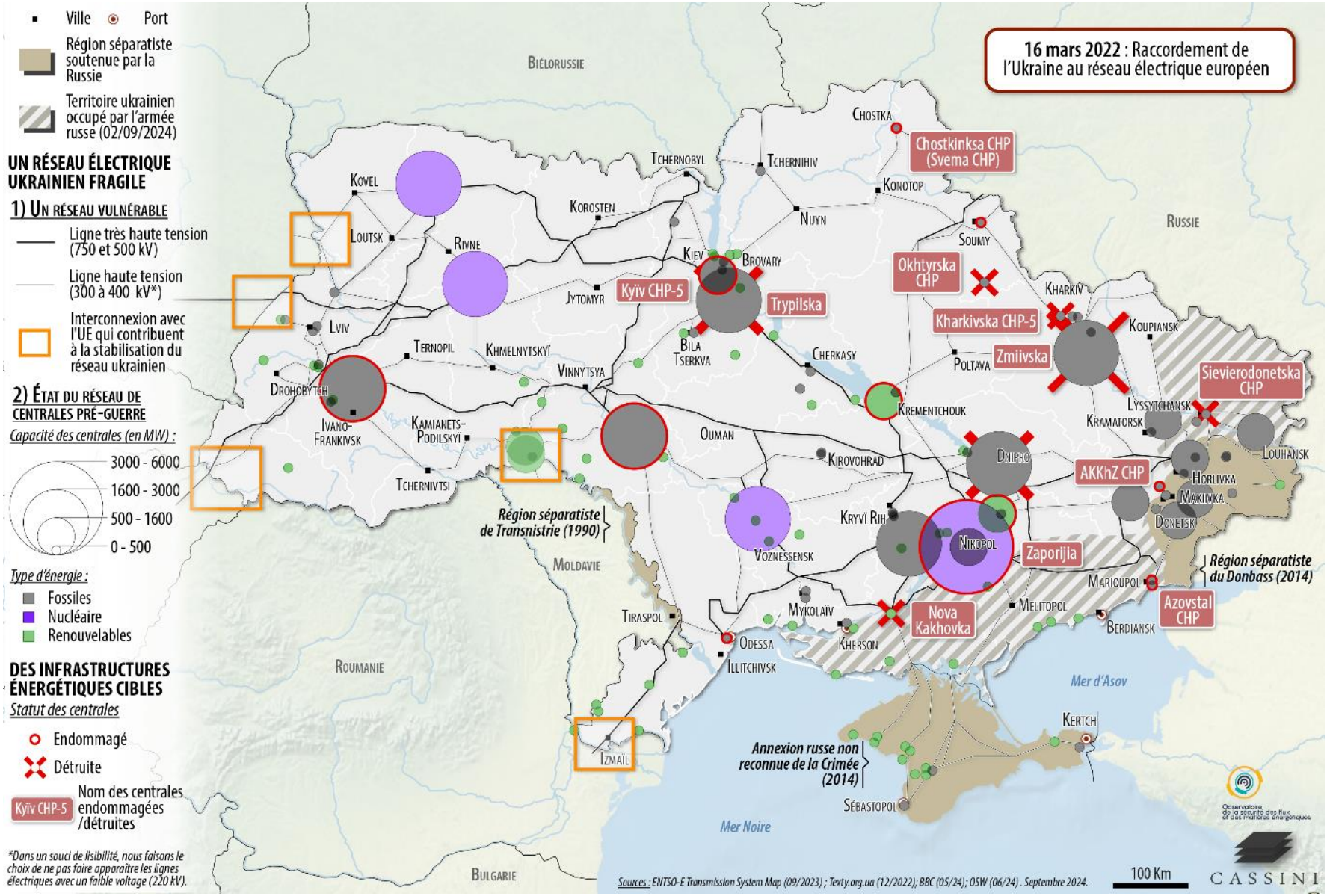
Avec 59 gigawatts de puissance installée, l'Ukraine comptait avant 2022 parmi les plus grands producteurs d'énergie en Europe et disposait d'importantes réserves de capacité. Désormais en déficit, il pourrait manquer de 7,5 à 5,8 GW à l'hiver 2024[9]. Plusieurs options sont alors envisagées pour gérer cette carence et renforcer la résilience du réseau ukrainien.

- Limitation de la consommation et coupures tournantes de façon à préserver l'approvisionnement des consommateurs critiques
- Renforcement de la défense antiaérienne
- Développement de capacités de production décentralisées
- Facilitation de l'acheminement de pièces de rechange ainsi que leur construction sur place
- Renforcement des interconnexions reliant l'UE à l'Ukraine

[8] Ukraine's computer emergency response team (CERT-UA), UAC-0133 (Sandworm) planifie le cyber-sabotage de près de 20 infrastructures critiques en Ukraine, 19 avril 2024. https://cert.gov.ua/article/6278706

[9] Susanne Nies, Oleh Savytskyi , « Six options to boost power transfers from Continental Europe to Ukraine, for the next two winters – Ukraine's power network integration with the EU », Green Deal Ukraina & Helmholtz Centrum (Berlin/Kyiv, Aout 2024), version mise à jour. https://greendealukraina.org/assets/images/reports/grid-solutions-ukraine-next-winters-final.pdf

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



CONCLUSION

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 :

1. 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.

2. 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.

3. 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.

4. 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