Brève n°93

Brève stratégique

Réseaux électriques et conflits

Mise en place et évolution des stratégies de résilience

INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE
irsem

Septembre **2026**

Angélique Palle

est géographe, chercheure associée à l'IRSEM ; elle travaille sur la géopolitique des transitions énergétiques et la sécurité climatique.

Les réseaux de transport d'électricité sont entrés au cœur des compétitions de puissance internationales. Ciblés aujourd'hui par la plupart des conflits armés mais aussi par les rivalités régionales autour de la fixation des normes et de l'accès aux ressources, ils font l'objet récent de stratégies de résilience diverses de la part des États.

Le 26 août 2026, le président Donald Trump déclare un état d'urgence nationale sur le réseau électrique américain, une mesure visant à empêcher l'achat de matériels électriques en provenance de Chine à destination du réseau américain. Cette déclaration, qui fait suite à plusieurs alertes du Department of Energy (DOE) et du Congrès sur la vulnérabilité de la chaîne d'approvisionnement du réseau électrique américain, vient entériner **15 ans d'entrée progressive des réseaux de transport d'électricité au cœur des compétitions de puissance internationales**.

Un ciblage généralisé par les conflits armés des infrastructures électriques, relativement inédit depuis la fin de la Seconde Guerre mondiale, est visible sur la scène internationale et s'étend à d'autres formes de rivalités. La guerre d'agression menée par la Russie en Ukraine est particulièrement emblématique de cette dynamique, et ce dès le premier jour du conflit (les forces russes franchissent la frontière alors que l'Ukraine mène un exercice d'isolation de son réseau du réseau russe, en vue de le raccorder à la plaque européenne). Elle se caractérise par une tentative de destruction généralisée du réseau ukrainien analysée dans un rapport de l'Observatoire de la sécurité des flux et des matières énergétiques à destination du ministère des Armées.

La stratégie ukrainienne de résilience repose alors sur plusieurs piliers. L'Ukraine cherche à décentraliser sa production pour la rendre moins vulnérable tout en multipliant les redondances d'un réseau actuellement surdimensionné pour la consommation effective du pays et en jouant sur sa connexion avec le réseau européen pour absorber les chocs des attaques russes. Un investissement technologique très important est réalisé dans la miniaturisation, la multi-connexion et la mobilité des centres de commande du réseau. Il s'accompagne inversement d'une très forte rusticité dans les interventions techniques de réparation du réseau, soutenues par l'approvisionnement en pièces d'équipement de ses alliés. Le mode dégradé dans la gestion des réparations du réseau est poussé à l'extrême (comparativement aux normes d'opération des réseaux européens auxquels l'Ukraine est connectée) pour maintenir l'accès à l'électricité de l'appareil industriel et de la population. La résilience de cette dernière est cruciale pour l'Ukraine et s'est accompagnée d'une stratégie de communication très aboutie du gestionnaire de réseau de transport d'électricité (GRT) ukrainien annonçant les coupures et les réparations, ainsi que de la mise en place d'abris d'urgence autonomes ou points d'invincibilité permettant l'accès à des services de base qui inspirent aujourd'hui l'Agence internationale de l'énergie et les plans de continuité de plusieurs États européens.

Hors d'Ukraine, le conflit au Moyen-Orient impliquant l'Iran, les États-Unis, Israël ainsi que plusieurs États voisins a lui aussi vu les infrastructures électriques régionales prises ouvertement pour cible au printemps 2026, tandis que l'embargo américain sur Cuba a largement contribué à provoquer un black-out global du réseau cubain en juillet dernier.

À ces offensives physiques sur les infrastructures électriques, se sont ajoutées depuis une vingtaine d'années des attaques cyber. En Europe, la première cyberattaque reconnue par un GRT a lieu en 2012 sur 50Hertz, l'un des GRT allemands. Le 23 décembre 2015, un black-out en Ukraine touche environ 225 000 consommateurs, il est attribué à une cyberattaque perpétrée par un groupe de hackers russes. C'est la première cyber attaque attribuée et officiellement reconnue comme réussie. En 2018, ce sont les systèmes américains et allemands qui annoncent subir des intrusions cyber. Les réseaux électriques font ainsi l'objet d'un suivi particulier des agences gouvernementales dédiées à la menace cyber, comme l'ENISA qui les analyse de façon complémentaire à d'autres infrastructures critiques comme les réseaux de télécommunications qui partagent des enjeux similaires.

Les acteurs visant les réseaux électriques ont également évolué, les compétitions de puissance impliquant des acteurs étatiques ou assimilés se combinent aujourd'hui à des actions menées à des échelles plus locales par des groupes d'opposition internes aux États. Ceux-ci ciblent les infrastructures électriques principalement pour des motifs politiques. Si les attaques menées à Berlin sur le réseau électrique en 2026 ont récemment médiatisé ces pratiques, la presse nationale et régionale française s'est fait l'écho d'une dizaine d'atteintes physiques contre le réseau français en dix ans. Elles comprennent des sciages de pylônes, des incendies de postes, certaines visant parfois des installations industrielles plus que le réseau lui-même ; plusieurs d'entre elles ont été revendiquées par des groupes se réclamant d'un militantisme anarchiste, écologiste ou d'extrême gauche.

À ces menaces d'origine humaine se greffent enfin les effets du changement climatique, déjà largement perceptibles en Europe. En renforçant l'ampleur et la fréquence des événements climatiques extrêmes, ils viennent ajouter une vulnérabilité supplémentaire à des réseaux électriques par ailleurs en cours de développement et de transformation. Les tempêtes hivernales, comme Ciaran, survenue en 2023 sur les côtes bretonnes, poussent les gestionnaires de transport et de distribution à adapter leurs infrastructures, tandis que les incendies, comme celui des Corbières dans l'Aude en 2026, et les sécheresses en été menacent les lignes mais aussi la stabilité de la production.

L'évolution de ces menaces et de ces vulnérabilités intervient dans un contexte de renforcement à la fois du rôle des infrastructures de transport électriques mais aussi de leur criticité. Alors que les États-Unis cherchent à consolider leur souveraineté sur leur réseau qui appelle d'importants investissements pour les années à venir, la Chine a mis le déploiement et le renforcement de son infrastructure électrique au premier plan de ses deux derniers plans quinquennaux. L'Union européenne suit la même dynamique et a annoncé un Paquet Réseau lors du *Clean Industrial Deal*. Actuellement en cours de négociation, il vise à soutenir, accélérer et sécuriser le déploiement des réseaux de transport d'électricité dans une double optique de respect des objectifs climatiques de l'UE fondée sur une électrification des usages, mais aussi de sortie de la dépendance européenne au gaz russe (l'UE a réduit officiellement ses importations de 150 bcm en 2021 à 36 bcm en 2025 ; des contournements avérés de la stratégie de réduction européenne, notamment du « blanchiment » d'origine via des pays tiers, sont cependant constatés rendant son efficacité globale difficile à évaluer).

Dans un secteur qui combine une forte inertie des infrastructures une fois déployées avec une grande rapidité d'évolution, les stratégies des acteurs pour assurer la sécurité de leur réseau diffèrent.

Les États-Unis ont un réseau vieillissant et peu maillé, qui souffre notamment des événements climatiques extrêmes mais aussi de défaillances techniques comme l'ont montré les black-out régionaux survenus ces dernières années (août 2026, Indiana ; décembre 2025, Ouest et Grandes-Plaines ; février 2025, Virginie ; mai 2025, Washington, Maryland et Virginie). Après plusieurs alertes sur la vulnérabilité globale du réseau américain (notamment celles de Jon Wellinghoff, ancien président de la Federal Energy Regulatory Commission) initiées depuis 2013 et l'attaque de l'un des postes électriques alimentant la Silicon Valley, la stratégie américaine, annoncée en août 2026 après plusieurs rapports du Congrès et du DOE américains sur les chaînes de valeur, se focalise sur le contrôle des approvisionnements. Elle vise entre autres à fermer à la Chine le réseau américain et particulièrement les onduleurs, transformateurs, systèmes de stockage par batteries et automates industriels.

La stratégie électrique chinoise comporte une dimension internationale de prise de contrôle des chaînes de valeur et des normes des composantes des réseaux électriques, ainsi que d'investissements ciblés dans les gestionnaires de réseaux de transport électrique internationaux. Par ailleurs, elle se focalise sur le renforcement et la protection du réseau national chinois. Perçu comme essentiel à l'industrie chinoise mais aussi à la transition énergétique et à la résilience climatique du pays, le réseau électrique national fait l'objet d'une attention particulière, notamment en ce qui concerne son indépendance vis-à-vis des importations extérieures et sa protection cyber.

Le réseau européen, contrairement au réseau américain, a cherché à construire une interconnexion forte, à l'échelle de l'Union et au-delà, depuis les années 1990. Il a servi de modèle à la construction du réseau chinois dont l'acteur principal, le gestionnaire de réseau State Grid, a d'ailleurs, depuis la crise de 2008, acquis des parts des réseaux portugais, grecs et italiens. Ce maillage européen rend les incidents majeurs plus rares mais plus importants lorsque des effets de chute d'infrastructures en cascade affectent le réseau. La stratégie européenne de développement et d'intégration du réseau a plus récemment intégré un volet de protection des infrastructures critiques, notamment sur le plan cyber. Il est porté par les directives NIS (*Network and Information System Security*) qui ont mis en place des normes transversales pour les infrastructures critiques dans un premier temps, dont les infrastructures énergétiques (NIS 1, 2016). Puis elles ont élargi le spectre des obligations de sécurité cyber, en particulier dans le secteur électrique, à l'ensemble des acteurs connectés aux réseaux et non à son seul gestionnaire (NIS 2, 2022). Ce renforcement de l'armature cyber du secteur électrique européen s'est accompagné de la mise en place d'exercices de gestion de crise spécifiques. Le CyberEurope 2024 de l'ENISA a ciblé pour la première fois le secteur de l'énergie européen, tandis que les exercices PENTEX, débutés à Paris en 2022, testent des scénarios de crise électrique à l'échelle régionale du Forum pentalatéral de l'énergie. Ce type d'exercice débuté il y a quelques années en UE, existe depuis 2011 aux États-Unis où les GridEx sont menés tous les deux ans.

angelique.palle@sciencespo.fr

IRSEM I École militaire
1, place Joffre, case 38
75700 Paris SP 07

irsem.fr