

Souveraineté nationale et cyberattaques

Madame le Commissaire enquêteur,

Un autre argument pour donner un avis défavorable à ce projet est apparu avec la guerre en UKRAINE : des éoliennes ont été touchées par une cyberattaque satellite, notamment en ALLEMAGNE, en BELGIQUE et en FRANCE.

Ces faits sont référencés sur le site de l'ARIA (DGPR – SRT – BARPI), la référence du retour d'expérience sur accidents technologiques de l'Etat :

- **N° 58778 - 24/02/2022 - FRANCE - 62 - COUPELLE-VIEILLE**

« Une cyberattaque du satellite de liaison entre le pilotage à distance et le système SCADA (Supervisory Control and Data Acquisition) des éoliennes entraîne la perte de surveillance et de contrôle à distance du parc éolien. »

<https://www.aria.developpement-durable.gouv.fr/accident/58778/>

- **N° 58714 - 24/02/2022 - FRANCE - - NC (= non communiqué)**

« Plus d'une cinquantaine de parcs éoliens français et d'autres en Europe sont touchés par une cyberattaque, affectant 30 000 éoliennes. Il s'agit de la perte de communication du pilotage à distance avec le système SCADA (Supervisory Control and Data Acquisition) des éoliennes. »

« Un mois après l'incident, tous les parcs ont retrouvé la communication à distance. »

<https://www.aria.developpement-durable.gouv.fr/accident/58714/>

- **N° 58868 - 01/04/2022 - FRANCE - 14 - ONDEFONTAINE**

Panne informatique dans un parc éolien :

« Vers 11h30, une perte de monitoring des éoliennes par le constructeur en charge de leur maintenance se produit sur un parc éolien. »

« Il s'agit d'une cyberattaque. »

<https://www.aria.developpement-durable.gouv.fr/accident/58868/>

Des cyberattaques sont relayées par la presse :

- **Le Figaro du 2 mars 2022 : « 6000 éoliennes allemandes touchées par une cyberattaque russe »**

« Quelques 6000 de ces installations ne répondent plus au pilotage à distance. Techniquement, elles fonctionnent en mode automatique, mais il n'est plus possible de les diriger à distance. Or, cette manœuvre s'avère indispensable en cas de vent supérieur à 80 km/h. La situation est d'autant plus dommageable qu'après presque une semaine, les experts mobilisés sur le sujet ne sont pas parvenus à redémarrer à distance les modems

affectés. La seule solution serait de les remplacer. Or, les stocks manquent, en raison de la pénurie de semi-conducteurs, notamment. »

<https://www.lefigaro.fr/secteur/high-tech/6000-eoliennes-allemandes-touchees-par-une-cyberattaque-russe-20220302>

- **Le Monde de l'informatique du 4 avril 2022 : « Le fabricant d'éoliennes NORDEX paralysé après une cyberattaque ».**

« L'étendue exacte de cette cyberattaque n'a pas été divulguée mais Nordex indique que les clients et les employés peuvent être impactés par l'arrêt de ses systèmes informatiques. Cet incident intervient après que, le 24 février 2022, la surveillance à distance et le contrôle de 5 800 turbines d'éoliennes d'un autre fabricant allemand Enercon (11Gw de puissance cumulée), a été perturbée par une panne de satellite causée par une attaque par déni de service en provenance, a priori, de Russie. »

<https://www.lemondeinformatique.fr/actualites/lire-le-fabricant-d-eoliennes-nordex-paralyse-apres-une-cyberattaque-86340.html>

- **Le Siècle digital du 27 avril 2022 : « Les éoliennes allemandes, nouvelles cibles des pirates russes ? »**

« Trois entreprises ont été touchées depuis le début du conflit en Ukraine, le 24 février, selon un décompte du Wall Street Journal. Enercon GmbH, spécialisée dans la fabrication de turbine et l'un des grands acteurs mondiaux de l'éolien, a été le premier visé. La commande de 5 800 éoliennes a été mise hors service dès les premières heures du conflit. »

« Les deux autres sociétés touchées par des cyberattaques ont, cette fois, été directement visées. Nordex, fabricant de turbines, et Windtechnik, société de maintenance, ont été toutes les deux victimes d'un rançongiciel le 31 mars et le 12 avril. Les deux ont dû couper leurs systèmes informatiques, dans le cas de WindTechnik le système de télécommande de 2 000 éoliennes a été coupé pendant un ou deux jours. »

<https://siecledigital.fr/2022/04/27/les-eoliennes-allemandes-nouvelles-cibles-des-pirates-russes/>

- **SEKURIGI – la sécurité informatique du 19 mai 2022 : « Un fabricant d'éoliennes, cible d'une cyberattaque ».**

« Au début du mois de mars, l'industrie énergétique allemande a été touchée par une cyberattaque russe de grande envergure. Dans les faits, 6000 éoliennes du fabricant d'éoliennes NORDEX ont subi une nouvelle attaque. »

« Nordex n'a pas divulgué l'étendue de l'attaque. Par contre, on a pu constater que bon nombre de produits de la Qrme ont connu des perturbations depuis qu'elle a affecté les éoliennes. Par ailleurs, l'arrêt de nombreux systèmes informatiques pour limiter la propagation de l'attaque s'est répercuté au niveau des clients et des employés. La fermeture des systèmes informatiques a aussi affecté les actionnaires de la société allemande NORDEX. Selon les responsables de NORDEX, il faudra des semaines pour rétablir la connexion et que les systèmes soient à nouveau opérationnels. De nouvelles informations seront apportées très prochainement, selon les responsables du fabricant d'éoliennes allemand, en fonction de l'avancement des travaux menés par l'équipe de réponse mise en place. »

*« Le secteur énergétique a un enjeu géostratégique majeur pour de nombreux pays. Dans le contexte de la guerre en Ukraine, l'industrie énergétique est une cible préférentielle dans cette confrontation. Avec la digitalisation et les connexions inter-réseaux, **ce secteur est devenu vulnérable aux cyberattaques**. Innovant sans cesse leurs approches, les cyberpirates ont recours à des méthodes de plus en plus élaborées pour perpétrer leurs attaques et causer le maximum de dégâts. »*

Ces risques graves sont d'importance pour qu'un avis défavorable s'impose.

Avec l'expression de mes sentiments distingués,

Edith de PONTFARCY