Monsieur le Commissaire-enquêteur,

A la suite de l'observation 261, donnons quelques exemples de cyberattaques visant des éoliennes et relayées dans la presse.

- **26 janvier 2026 – BFMTV : « *La Pologne a-t-elle frôlé un black-out national ? Une cyberattaque attribuée à des hackers russes a visé le réseau électrique avec un puissant logiciel malveillant "wiper" inédit* »**

*https://www.bfmtv.com/tech/cybersecurite/la-pologne-a-t-elle-frole-un-black-out-national-une-cyberattaque-attribuee-a-des-hackers-russes-a-vise-le-reseau-electrique-avec-un-puissant-logiciel-malveillant-wiper-inedit_AN-202601260424.html*

« *Des chercheurs ont ainsi révélé vendredi que le réseau électrique polonais avait été visé par un logiciel malveillant de type "wiper", probablement déployé par des hackers liés à l'État russe, avec pour objectif de perturber la distribution d'électricité. Selon Reuters et Ars Technica, l'attaque, survenue à la fin du mois de décembre, cherchait à* ***désorganiser les communications entre les installations d'énergies renouvelables et les gestionnaires du réseau***. »

- **30 avril 2025 – OUEST-France : « *En mer, les éoliennes sont aussi vulnérables aux cyberattaques* »**

https://www.ouest-france.fr/economie/energie/energie-eolienne/en-mer-les-eoliennes-sont-aussi-vulnerables-aux-cyberattaques-8c4745b6-2514-11f0-8e4d-80235dd3728c

« *Deux organisations du secteur maritime s'allient pour renforcer la cybersécurité des champs éoliens.* ***Ceux-ci peuvent être la cible de hackeurs « opportunistes » ou de déstabilisation étatique.*** »

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

https://www.sekurigi.com/2022/05/un-fabricant-deoliennes-cible-dune-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 firme 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. »*

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

https://siecledigital.fr/2022/04/27/les-eoliennes-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. »*

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

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

*« **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. »*

- **2 mars 2022 – TF1info : Les éoliennes de France menacées par les cyberattaques ?**

https://www.tf1info.fr/high-tech/video-guerre-en-ukraine-les-eoliennes-de-france-menacees-par-les-cyberattaques-de-la-russie-2212347.html

*« En parallèle de son invasion de l'Ukraine, la Russie mène, depuis plus d'une semaine, de multiples opérations sur Internet. »*

« ***Des infrastructures dans l'Europe entière sont ciblées, et notamment certains parcs éoliens.*** »

- **3 mars 2022 – PV Magazine : *« Une cyberattaque sur un satellite affecte 11 GW d'éoliennes allemandes »***

https://www.pv-magazine.fr/2022/03/03/une-cyberattaque-sur-un-satellite-affecte-11-gw-deoliennes-allemandes/

*« La défaillance des systèmes de contrôle des convertisseurs des éoliennes pourrait être le dommage collatéral d'une cyberattaque menée sur une cible militaire lors de l'attaque de l'Ukraine par la Russie le 24 février dernier, car* ***les éoliennes utilisent les mêmes canaux de communication par satellite que l'armée américaine***. »

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

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

« ***Quelque 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.* »

Force est de constater la vulnérabilité du mode production énergétique à partir de l'éolien.

Un avis défavorable ne peut qu'être requis.

Avec mes salutations distinguées,

Edith de PONTFARCY