# Souveraineté nationale et cyberattaques

Monsieur le commissaire enquêteur,

Un argument majeur pour donner un AVIS TRÈS DÉFAVORABLE à ce projet apparaît à la lecture du dossier d'enquête publique unique à la demande de permis de construire d'un parc photovoltaïque déposée par la société Parc Solaire de Cressia filiale de la société RWE Renouvelables France sur le territoire de la commune de Cressia.

Il s'agit de l'**omission du risque de cyberattaques** alors qu'il est bien réel, même si depuis le début de la guerre en Ukraine, l'information le concernant est devenue confidentielle.

Voici quelques informations à ce sujet.

26 Août 2024 - Les panneaux photovoltaïques pourraient bien constituer le talon d'Achille de la sécurité énergétique de l'Europe, du fait de leur vulnérabilité aux cyberattaques. En cause : les convertisseurs de ces panneaux, souvent connectés à internet, mais mal dotés en matière de cybersécurité. Un hacker néerlandais, qui est parvenu à prendre le contrôle de millions de panneaux, sonne l'alerte.
https://www.revolution-energetique.com/des-millions-de-panneaux-solaires-pirates-par-un-gentil-hacker-explications/

[Traduction] 22 août 2023 - La cyberattaque met en évidence les préoccupations en matière de sécurité du réseau énergétique.
Quelques jours seulement après qu'un organisme de recherche financé par le gouvernement fédéral ait mis en garde contre les cyberrisques potentiels pour les réseaux énergétiques australiens en raison de la technologie solaire de fabrication étrangère, le fournisseur de logiciels d'énergie en gros Energy One, dont le siège social de Sydney a subi une violation de données.
Le fournisseur de logiciels énergétiques Energy One coté à ASX a été ciblé dans une cyberattaque confirmant que «certains systèmes d'entreprise en Australie et au Royaume-Uni» ont été affectés.
https://www.pv-magazine-australia.com/2023/08/22/cyberattack-highlights-energy-grid-security-concerns/

30 mai 2023 – Failles 'Les panneaux solaires souvent facilement piratables via internet'
Une recherche effectuée sur divers onduleurs montre que les panneaux solaires sont souvent faciles à pirater. Voilà la teneur de la mise en garde lancée par la Rijksinspectie Digitale Infrastructuur (RDI), le régulateur néerlandais des communications.
https://datanews.levif.be/actualite/securite/failles/les-panneaux-solaires-souvent-facilement-piratables-via-internet/

18 décembre 2020 - Cyber-attaque : le département fédéral américain de l'énergie victime du piratage Sunburst.
Le département américain de l'énergie est la dernière agence à confirmer qu'il a été la cible de ce qui est décrit comme le pire piratage jamais commis contre le gouvernement américain.
*Le département est responsable de la gestion des armes nucléaires américaines, mais a déclaré que la sécurité de l'arsenal n'avait pas été compromise.*

C. RECEVEUR – février 2025

*Note du rédacteur :* Sunburst est un ***malware*** qui a été utilisé dans une ***attaque par supply chain*** contre l'entreprise ***SolarWinds***. Cette attaque a été découverte en décembre 2020 par la société de cybersécurité ***FireEye***. Le *malware* a été intégré dans une version officielle d'un logiciel de gestion réseau édité par *SolarWinds*, ce qui a permis aux attaquants d'accéder aux systèmes de nombreux clients de *SolarWinds*. On estime que ***18 000*** organisations *ont été touchées par cette attaque.*
https://www.bbc.com/afrique/monde-55363091

[Traduction] 31 octobre 2019 - La société d'énergies renouvelables de l'Utah a été frappée par une rare cyberattaque en mars
Une entreprise d'énergie renouvelable basée dans l'Utah a été victime d'une rare cyberattaque qui a temporairement perturbé les communications avec plusieurs installations solaires et éoliennes en mars, selon des documents obtenus en vertu de la loi sur la liberté de l'information.
https://cyberscoop.com/spower-power-grid-cyberattack-foia/

« ***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.* »

**Comment un tel risque a pu être ignoré par le porteur de projet ? La sécurité de fourniture d'électricité en France et sa souveraineté ne peuvent se satisfaire d'une telle légèreté de l'étude.**

Ce risque grave est d'importance pour qu'un **AVIS TRÈS DÉFAVORABLE** s'impose.