Cyberattaques : les éoliennes sont vulnérables

Deux organisations s'allient pour renforcer la cybersécurité des champs éoliens, qui peuvent être la cible de hackeurs « opportunistes » ou de déstabilisation étatique.

En France, trois parcs éoliens en mer sont opérationnels à ce jour : Saint-Nazaire (Loire-Atlantique), Fécamp (Seine-Maritime) et Saint-Brieuc (Côtes-d'Armor). D'ici à 2050, l'objectif du gouvernement est que l'électricité issue de l'éolien en mer passe d'environ 2 % aujourd'hui à environ 30 %.

Trois nouveaux parcs sont en construction et devraient être mis en fonctionnement cette année (Courseulles-sur-Mer, dans le Calvados, et Yeu-Noirmoutier, en Vendée) et 2026 (Dieppe-Le Tréport, en Seine-Maritime). Ces fermes éoliennes sont, au même titre que les centrales nucléaires, des infrastructures stratégiques, car elles contribuent au système énergétique français.

Le parc éolien en baie de Saint-Brieuc (Côtes-d'Armor). | PHOTO : G. SALIGOT. ARCHIVES O.-F.

Une numérisation accrue

« Il faut être capable de les protéger sur le plan physique, mais aussi sur le plan numérique », déclare Jean-François Filipot, directeur scientifique de France énergies marine (Fem), un centre de recherche sur l'éolien en mer basé à Brest (Finistère). Fem vient de nouer un partenariat avec France cyber maritime, une association brestoise qui vise à renforcer la cybersécurité du secteur maritime.

L'essor des éoliennes en mer s'accompagne aussi d'une numérisation accrue. Beaucoup d'actions sont contrôlées à distance : le démarrage et l'arrêt des machines, la vitesse et l'angle des pales, qui vont déterminer la puissance de la machine et donc l'énergie qui va pouvoir être vendue. **« On récupère aussi pas mal de données numériques des fermes sur l'état de santé des machines,** poursuit Jean-François Filipot. **Ça permet de mieux planifier les opérations de maintenance. »**

« Les cyberattaques se sont multipliées ces dernières années et des secteurs qui n'étaient pas touchés commencent à l'être, explique Xavier Rebour, directeur de France cyber maritime. **Il n'y a pas eu d'attaques sur les champs éoliens en France, mais le secteur n'était pas développé. On en a vu en Allemagne ou au Danemark. »**

Hackeurs « opportunistes » ou étatiques

Deux types de cyberattaques sont envisageables. D'abord, les cybercriminels : celles de hackeurs « opportunistes » qui bloquent les parcs à distance pour demander une rançon. **« C'est une perte sèche pour l'opérateur. Et c'est parfois la double peine, parce qu'il peut y avoir un vol de données. Si on paie une fois, le cybercriminel peut se dire que l'opérateur va repayer pour que ses données ne soient pas vendues sur Internet. Il n'est pas conseillé de payer la rançon, il vaut mieux se protéger avant. »**

Autre type de menace : les attaques étatiques ou para-étatiques. **« C'est beaucoup plus insidieux, parce que ce n'est pas pour demander une rançon, c'est pour perturber la production d'électricité. »**

Le partenariat entre France énergies marines et France cyber maritime a plusieurs objectifs. Tout d'abord, **« mettre autour d'une table des constructeurs de champs d'éoliens et des entreprises de cybersécurité. Elles vont pouvoir travailler ensemble sur les turbines en elles-mêmes, mais aussi l'écosystème d'un parc depuis sa construction et jusqu'au raccordement à terre, en passant par la surveillance à distance. »**

Ensemble, les deux organisations vont rédiger un livre blanc sur la cybersécurité de l'éolien en mer, avec le Syndicat des énergies renouvelables, mettre en place des formations et référencer les entreprises expertes en cybersécurité pour l'éolien offshore.

Emmanuelle FRANÇOIS.