SÉCURITÉ DES INFRASTRUCTURES ÉNERGÉTIQUES RENOUVELABLES EN FRANCE : NOUVEAUX DÉFIS DE LA TRANSITION ÉNERGÉTIQUE

La transition énergétique en France représente un défi majeur pour atteindre les objectifs de neutralité carbone d'ici 2050. À mesure que le pays passe des énergies fossiles aux énergies renouvelables, la sécurisation des infrastructures de production, de transport et de stockage devient primordiale. Les énergies renouvelables, bien que cruciales pour réduire l'empreinte carbone, présentent de nouvelles vulnérabilités face aux risques de malveillance, de cyberattaques et d'événements climatiques extrêmes.

Cet article a le mérite d'explorer l'impact de ces défis sur la sécurité publique et les infrastructures énergétiques, tout en analysant les solutions mises en place pour les contrer.

À la lumière de tout ce qui précède, il convient d'étudier d'une part, les vulnérabilités des réseaux énergétiques renouvelables (I) et d'autre part, les réponses sécuritaires aux nouvelles menaces (II).

I-LES VULNÉRABILITÉS DES RÉSEAUX ÉNERGÉTIQUES RENOUVELABLES

Les infrastructures d'énergie renouvelable sont aujourd'hui de nouvelles cibles pour des actes de malveillance (a) et subissent également les impacts des catastrophes naturelles (b).

a-LES NOUVELLES CIBLES DE LA MALVEILLANCE

L'un des défis majeurs pour la sécurité des infrastructures renouvelables réside dans leur fragilité face aux actes de malveillance. En France, les infrastructures énergétiques critiques sont de plus en plus ciblées par des cyberattaques (Ransomwares) et des actions de sabotage. Les parcs éoliens, les centrales solaires et même les réseaux de stockage d'énergie deviennent des cibles potentielles pour des groupes radicaux ou des acteurs étatiques étrangers cherchant à perturber la transition énergétique.

De ce fait, en 2023, un parc éolien situé en Bretagne a été victime d'une cyberattaque, qui a perturbé l'accès à son système de gestion à distance, rendant l'optimisation de la production d'énergie temporairement impossible. Bien que cet incident n'ait pas causé de dommages majeurs à la production d'énergie, il a mis en évidence les vulnérabilités croissantes des infrastructures face aux menaces numériques.

En outre de ces actes de malveillance à l'égard des installations d'énergie renouvelable, ces dernières subissent aussi des conséquences néfastes engendrées par des catastrophes naturelles.

b-LES IMPACTS DES CATASTROPHES NATURELLES

Les événements climatiques extrêmes, de plus en plus fréquents en raison du changement climatique, représentent également un danger considérable pour les infrastructures énergétiques. Des tempêtes, des inondations ou des incendies peuvent endommager les équipements et perturber l'approvisionnement énergétique. Par exemple, la tempête **CIARA** en février 2020 a endommagé des centaines d'éoliennes en mer au large de la côte bretonne, augmentant les coûts de maintenance et réduisant temporairement la capacité de production.

En outre, l'élévation du niveau des mers pourrait, dans les années à venir, menacer les installations offshore[1], qui constituent un pilier de la production d'énergie en France, notamment en **Bretagne** et en **Normandie**.

II-LES RÉPONSES SÉCURITAIRES AUX NOUVELLES MENACES

Ces réponses se traduisent par la mise en place des dispositifs de surveillance et de prévention (a) et d'une collaboration privée-publique (b).

a-DES DISPOSITIFS DE SURVEILLANCE ET DE PRÉVENTION

Pour contrer ces risques, des mesures de sécurité renforcées ont été déployées. L'**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation (**ANSSI**) joue un rôle clé dans la sécurisation des réseaux énergétiques, avec un accent particulier sur la

[1] **Les installations offshore** sont des infrastructures situées en mer, utilisées pour produire de l'énergie, comme les éoliennes ou les plateformes pétrolières.

cybersécurité des infrastructures critiques. Des systèmes de surveillance sophistiqués, tels que **les drones de surveillance** et **les capteurs intelligents**, sont utilisés pour détecter des comportements suspects autour des sites de production.

En 2022, un projet pilote a été lancé dans les **Hauts-de-France** pour installer des capteurs connectés sur des éoliennes afin de détecter tout mouvement anormal. En 2021, l'opérateur **EDF** a installé un système de surveillance par drones sur les centrales solaires de Provence, ce qui a permis de détecter une tentative de sabotage avant qu'elle ne puisse causer des dommages significatifs. Cette initiative a été étendue à d'autres sites critiques.

À part l'instauration de ces mécanismes de protection, toujours dans cette même optique, il y a aussi le recours à un Partenariat Privé-Public (PPP) pour plus d'efficacité des infrastructures.

b-LA COLLABORATION PRIVÉE-PUBLIQUE

Le partenariat entre le secteur privé et public est indispensable pour renforcer la sécurité des infrastructures énergétiques renouvelables. Le gouvernement français a lancé en 2022 un **Plan National de résilience des infrastructures critiques**, **incluant un volet spécifique pour les énergies renouvelables**. Ce plan encourage une collaboration renforcée entre les opérateurs privés d'énergie et les autorités publiques pour garantir la sécurité des installations.

En **Bretagne**, des exercices conjoints entre les forces de gendarmerie et les opérateurs d'éoliennes ont été organisés en 2023. Ces simulations ont permis de tester les protocoles d'intervention rapide en cas de malveillance, renforçant ainsi la capacité de réaction face à toute tentative de perturbation.

CONCLUSIONS:

La sécurité des infrastructures d'énergie renouvelable est un enjeu crucial en pleine transition écologique. Face aux menaces croissantes, qu'elles soient d'origine humaine (malveillance, cyberattaques) ou environnementales (intempéries, catastrophes naturelles), il est impératif d'adopter une approche proactive pour garantir leur résilience et leur bon fonctionnement. L'essor des énergies renouvelables ne doit pas se faire au détriment de la sûreté des installations, sous peine de mettre en péril la continuité de l'approvisionnement énergétique et

la confiance des citoyens dans ces nouvelles technologies. À cet effet, voici quelques recommandations :

1. Renforcer la cybersécurité des infrastructures

- Développer des systèmes de protection avancés contre les cyberattaques, notamment via l'intelligence artificielle et la cryptographie.
- Exiger des audits de sécurité réguliers pour toutes les installations connectées aux réseaux intelligents (smart grids).

2. Protéger les sites sensibles contre les actes de malveillance

- Mettre en place des dispositifs de surveillance renforcée (vidéoprotection, drones, capteurs intelligents) sur les sites les plus stratégiques.
- Renforcer la coopération entre les opérateurs énergétiques et les forces de l'ordre pour mieux prévenir les intrusions et sabotages.

3. Adapter les infrastructures aux risques climatiques

- Concevoir des équipements capables de résister aux conditions météorologiques extrêmes (vent violent, montée des eaux, tempêtes).
- Investir dans des matériaux plus résistants et des systèmes d'ancrage renforcés pour les installations offshore.

4. Améliorer la coordination entre les acteurs publics et privés

- Créer une cellule de crise dédiée à la protection des infrastructures énergétiques renouvelables, impliquant les autorités publiques et les industriels.
- Développer des protocoles d'urgence pour garantir une réaction rapide en cas d'attaque ou de catastrophe naturelle.

5. Sensibiliser et former les professionnels du secteur

- Intégrer des modules de formation sur la sûreté et la gestion des risques pour les ingénieurs et techniciens travaillant sur ces infrastructures.
- Organiser des exercices de simulation pour tester la réactivité des exploitants face aux menaces.

En adoptant ces mesures, la France pourra garantir une transition énergétique sécurisée et pérenne, tout en minimisant les risques liés aux infrastructures d'énergie renouvelable.

Sources et liens URL [2]: Ecologie.gouv.fr ; The Good FAB ; It social ; ANSSI ; TNP

Anonyme

[2] https://www.ecologie.gouv.fr/sites/default/files/documents/Volets%20Sécurité%20d%27approvisionnement%20-%20infrastructures.pdf

https://www.thegoodfab.com/post/securite-energetique-en-france-defis-et-perspectives-pour-les-entreprises

https://itsocial.fr/contenus/tribunes/energie-renouvelable-veiller-a-la-cybersecurite-energetique-de-demain/

https://www.ecologie.gouv.fr/sites/default/files/documents/23242_Strategie-energie-climat_def2_0.pdf

https://cyber.gouv.fr/sites/default/files/2022-08/rapport_annuel_anssi_2016%5B1%5D.pdf

https://www.tnpconsultants.com/blog-la-cybersecurite-volet-incontournable-de-la-transition-energetique/