Die NATO ist entschlossen, wichtige Unterwasser-Energieinfrastruktur zu schützen

geschrieben von Andreas Demmig | 31. Dezember 2024

Einleitung
Hier ein Bericht über die Absichten, wichtige Energie-Infrastruktur, insbesonders auch in der Ostsee zu schützen. Schade, dass dieses Abkommen noch nicht am 26. September 2022, Sprengung von Nordstream II in Kraft war?

Wind Europe.org, 19. Dezember 2024

Europa möchte viel mehr erneuerbare Energien nutzen, um seine Energiesicherheit und industrielle Wettbewerbsfähigkeit zu stärken. Die geopolitische Lage wirft neue Fragen zur Sicherheit dieser Anlagen auf. Bei seinem jährlichen Runden Tisch zur Energiesicherheit bekräftigte die NATO ihre Entschlossenheit, kritische Energieinfrastrukturen zu schützen.

Der Krieg in der Ukraine hat die Bedrohungslandschaft in ganz Europa, insbesondere in der Ostsee und im Arktischen Ozean, radikal verändert. Diese Woche veranstaltete die NATO im NATO-Hauptquartier in Brüssel ihren jährlichen Runden Tisch zur Energiesicherheit. WindEurope-CEO Giles Dickson nahm an einer Podiumsdiskussion über kritische Energieinfrastruktur auf See und allgemeinere Bedrohungen der Energiesicherheit teil.

Schutz von Turbinen und Netzen vor feindlichen Sabotageakten und Cyberkrieg

Das NATO-Gremium konzentrierte sich auf aktuelle physische und Cybersicherheitsbedrohungen für Offshore-Windparks und Unterseekabel. Es kam zu dem Schluss, dass hybride Angriffe und Sabotage weiterhin die dringendsten Bedrohungen für die kritische Unterseeinfrastruktur in Europa darstellen. Dickson betonte auch die entscheidende Bedeutung der Datensicherheit.

> *„Europa muss seine Bemühungen verstärken, seine wachsende Offshore-Windinfrastruktur vor physischen Angriffen und Sabotage zu schützen. Gleichzeitig dürfen wir die Bedrohungen für die Cyber- und Datensicherheit nicht unterschätzen. An einer modernen Windturbine befinden sich 300 Sensoren. Die Daten dieser Sensoren sollten ausschließlich in Europa und befreundeten Ländern gespeichert und analysiert werden“,* sagte Dickson.

NATO-Außenminister warnen vor feindlichen Aktionen Russlands und Chinas

Das Ereignis fand eine Woche nach dem Treffen der NATO-Außenminister in Brüssel statt, bei dem es um die eskalierenden Feindseligkeiten in NATO-Ländern ging. Bei der Vorstellung der Ergebnisse dieses Treffens sagte NATO-Generalsekretär Mark Rutte: „Sowohl Russland als auch China haben versucht, unsere Länder zu destabilisieren und unsere Gesellschaften durch Sabotageakte, Cyber-Angriffe und Energieerpressung zu spalten."

Auch die NATO-Außenminister wiesen auf einen starken Anstieg solcher Angriffe hin. „In diesem Jahr gab es in Europa 500 verdächtige Vorfälle. Bis zu 100 davon können auf russische Hybridangriffe, Spionage und Einflussnahme zurückgeführt werden", sagte der tschechische Außenminister Jan Lipavsky.

Auf ihrem Gipfeltreffen in Vilnius 2023 einigte sich die NATO darauf, ein maritimes Zentrum für die Sicherheit kritischer Unterwasserinfrastrukturen (CUI) innerhalb des NATO-Marinekommandos (MARCOM) einzurichten. Diese CUI-Koordinationszelle wurde 2023 einsatzbereit. Ihr Schwerpunkt liegt auf der Abschreckung und Abwehr des Zwangseinsatzes von Energie und anderer hybrider Aktionen. Sie bündelt auch die Satellitenüberwachung feindlicher Schiffe, die möglicherweise die Energieinfrastruktur beeinträchtigen. Bei dem Treffen der NATO-Außenminister wurden ein verstärkter Informationsaustausch, gemeinsame Übungen, ein besserer Schutz kritischer Infrastrukturen und die Cyberabwehr diskutiert.

Wind erhöht die Energiesicherheit

Windenergie deckt mittlerweile 20 % des gesamten europäischen Stromverbrauchs. Sie ist für die Stärkung der Energiesicherheit Europas von entscheidender Bedeutung. Nicht zuletzt, weil sie heimisch ist und den Bedarf an Importen fossiler Brennstoffe verringert. Die Windenergie, die in diesem Jahr erzeugt wurde, hat Europa das Äquivalent von 100 Milliarden Kubikmetern Gasimporten erspart.

Die dezentrale Natur der Windenergie – in ganz Europa gibt es 107.000 Windräder – macht sie zudem weniger anfällig für Sabotage und ausländische Einmischung als viele andere Energieformen. Die Bundeswehr rät deutschen Unternehmen mittlerweile, eigene Windräder zu betreiben.

Aber auch Wind- und Netzanlagen müssen geschützt werden

Die physischen Bedrohungen für Europas Wind-, Strom- und sonstige Offshore-Energieinfrastruktur sind real. Dasselbe gilt für die Cyber- und Datenbedrohungen für die Windenergieinfrastruktur an Land und auf See.

Moderne Windkraftanlagen sind mit bis zu 300 Sensoren ausgestattet, die die Leistung der verschiedenen Komponenten überwachen. Diese Sensoren produzieren riesige Datenmengen und ermöglichen die Steuerung der Funktionsweise der jeweiligen Komponenten und damit der Turbinen. Es ist wichtig, die damit verbundenen Risiken zu mindern und eine maximale

Datensicherheit der europäischen Windparks zu gewährleisten. Und sie vor Cyberangriffen zu schützen. Dies erfordert Verschlüsselungstools, sichere SCADA-Systeme und EU-basierte Datenmanagementlösungen.

Der EU Cyber □□Resilience Act, die „NIS2“-Richtlinie (das Cybersicherheitsgesetz der EU) und der EU-Netzwerkkodex für Cybersicherheit sind hier wichtige Instrumente. Der EU Net Zero Industry Act schreibt außerdem Vorqualifizierungskriterien bei Windenergieauktionen hinsichtlich Cyber- und Datensicherheit vor.

https://windeurope.org/newsroom/news/nato-determined-to-protect-critical-undersea-energy-infrastructure/