Save Long Beach Island, Inc. (Save LBI)
PO Box 2087
Long Beach Township, NJ 08008
www.savelbi.org

Issue Paper: Offshore Wind and Critical Infrastructure Security

For years, Save LBI has exposed the serious impacts of offshore wind development on marine mammals, fisheries disruption, visual impacts, economic cost and national security regarding impairment of our onshore military radars. There is another issue that deserves equal scrutiny:

Is it strategically sound to place a growing share of our electric-generation infrastructure in a remote, exposed, and difficult-to-defend offshore environment?

Offshore wind installations are not just turbines. They are interconnected industrial control systems, underwater transmission cables, offshore substations, satellite-linked monitoring systems, and remote maintenance platforms. In national infrastructure terms, they are distributed critical assets—highly visible, highly networked, and inherently exposed.

Cyber Vulnerabilities Are Real

Recent research from Concordia University and Hydro-Québec Research Institute found that offshore wind systems using high voltage-direct current (HVDC) converter technology create multiple cyberattack entry points. Researchers concluded that compromised sensor data or communications could destabilize power output and potentially affect the broader grid. (ScienceDaily)

The U.S. Department of Energy has also published warnings that wind energy systems are increasingly targets of cyberattacks, with incidents already documented in multiple countries. Their findings emphasize vulnerabilities in supervisory control and data acquisition (SCADA) systems, vendor software, and remote access pathways, (https://www.energy.gov/cmei/systems/articles/protecting-wind-energy-systems-cyberattacks)

The World Economic Forum, working with industry leaders including Accenture reports that 64% of energy-sector professionals believe their infrastructure is more vulnerable to cyber threats than ever before. Offshore wind's dependence on continuous digital connectivity increases that exposure. (https://www.weforum.org/publications/global-cybersecurity-outlook-2026/)

Physical Sabotage Is Not Hypothetical

Offshore installations are geographically isolated and difficult to defend at scale. They present obvious targets for:

- **Drone attacks** against transformers, blades, or offshore substations
- **Sabotage of offshore substations**
- **Underwater sabotage** of export cables or seabed infrastructure
- **GPS spoofing (signal manipulation)** affecting maintenance and monitoring vessels
- **Coordinated maritime incursions** exploiting turbine fields as operational cover

Europe's recent concern over attacks on undersea pipelines and communications cables has heightened awareness of how vulnerable offshore infrastructure can be to state-backed sabotage. Germany now requires certain offshore wind farms to install radar systems to improve maritime security monitoring. (https://www.marinelink.com/blogs/blog/german-wind-farms-are-asked-to-install-radar-due-to-security-102618)

Hard Questions Need Answers

Before expanding offshore wind at scale, communities and regulators should demand clear answers:

- Who is responsible for defending these installations in a hostile event?
- What are the contingency plans for prolonged outages caused by cyber or physical attack?
- How vulnerable are offshore substations and underwater transmission cables?
- What percentage of regional power could be lost if one major offshore installation were disabled?
- Are taxpayers ultimately underwriting the security risks?

The Bottom Line

Planning for electric generation infrastructure must consider not only reliability, cost, longevity and environmental impact—but in today's world- its physical vulnerability to attack.

The question is simple:

Should critical electric-generation assets be concentrated in environments that are remote, digitally dependent, physically exposed, and difficult to defend?

Before committing billions more to offshore wind, the public deserves a full national-security risk assessment—not after deployment, but before.

Save LBI has asked the Department of War (DOW) to revisit its Memorandum of Understanding with the Interior Department to assure that offshore wind projects are compatible with DOW responsibilities regarding both radar performance and critical structure vulnerability.