Use Case and Requirements Specification and Wind Farm Threat Landscape

September 2026

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

AENAON

Work Package	WP2 Requirements Specification, Federated Digital Twin-based Cyber Range Platform Set up and Interactive Training Programme Development
Lead author	WINDE
Contributors	All WP2 participants
Peer reviewers	CLX, SAG, MORE
Version	V1.0

About

AENAON develops a Federated Digital Twin-based Cyber Range platform to improve cybersecurity preparedness and resilience of offshore wind farms across Europe. Funded by the Digital Europe Programme through the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC),

aenaon-project.eu

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC).

Keywords

Offshore wind cybersecurity; use case specification; requirements specification; cyber threat landscape; offshore wind farms; operational technology (OT); industrial control systems (ICS); SCADA; remote access compromise; supply chain risk; OEM dependency; ransomware; wiper malware; DDoS; AI-enabled threats; threat actors and adversaries; open-source intelligence (OSINT); cyber resilience; critical energy infrastructure; EU energy security; NIS2 Directive; Cyber Resilience Act; digital twin; cyber range; managed security services; AENAON.

Disclaimer

This document contains information which is proprietary to the AENAON consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or parts, except with the prior written consent of the AENAON consortium.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Table of contents

1. Executive Summary 8

2. List of figures 10

3. List of tables 10

4. Acronyms & Abbreviations 11

5. Introduction 16

Scope & Sector Definition 16

Reporting period 17

Target audience 17

Intelligence Requirements & Key Questions 17

Methodology Overview 18

Open-source intelligence 20

Surveying Offshore Wind Industry 21

6. Offshore Wind Use Case Foundations & Sector Context 23

Role of Wind Energy in EU Energy Security 23

Regulatory Landscape 24

The Network and Information Security (NIS2) Directive 25

The EU Cyber Resilience Act (CRA) 26

General Data Protection Regulation 27

EU AI Act 27

EU Data Act 27

An Evolving Regulatory Landscape 28

Reference Digital Architecture of the Offshore Wind Use Case 29

General Description 29

Network segments 30

Substation Protection Network 31
CCTV/ Alarm Network 31
Bird Detection System Network 31
Peripheral Stakeholders 32
AENAON Reference Offshore Wind Use Case 34

7. Threat Landscape Overview 35
Summary of Observed Incidents 35
Stakeholder threat perception 38
Digital Exposure & Critical Dependencies 38
Threat Perception 39
Preparedness & Capability Gaps 39
Sector-Level Vulnerability 40
Energy, Defence and the Wider Sample 40
Comparison with Observed Incidents 40

8. Primary Threats 42
Distributed Denial-of-Service (DDoS) 42
Intrusion & Data-Related Threats 43
Ransomware 45
Supply Chain Compromise 46
OT/ ICS Targeted Attacks 47
Insider & Credential Abuse 49
Wiper 50
AI-Enabled Threats 51

9. Key Adversaries 56
State-Nexus Intrusion Sets 56
Cybercrime operators 57
Hacktivists 59
Hybrid & Information Operation Actors 61

10. Attack Surface & Supply Chain Dependencies 65

ICT Supply Chain of Offshore Wind 65

Third-Party & Vendor Exposure 67

Remote Access & Maintenance Channels 68

11. Impact Analysis 70

Operational Disruption 70

Grid Stability & Cross-border Implications 71

Safety & Environmental Impact 73

Cyber-to-physical impact pathways 74

Impact prioritisation 75

Implications for AENAON preparedness 75

Reputational & Economic Impact 76

12. Outlook (12-24 months) 78

Expected Evolution of Threat Types 78

Geopolitical Risk Drivers 80

Emerging Technical Risks 81

Regulatory and Compliance Implications 84

13. Recommendations 87

Policy Recommendations 87

Preparedness, Exercises and Sector Coordination 87

Operator and Supplier Measures 88

References 89

Appendix A – Detailed Methodology 96

Intelligence Direction 96

Collection Phase 97

Processing & Taxonomy 98

Analytical techniques 98
Limitations 99

Appendix B – Baseline legal obligations under NIS2 and CRA 103

Appendix C - Initial AENAON Requirements Baseline 109

Purpose and interpretation 109
Review and refinement process 114

1. Executive Summary

This report provides a structured assessment of the cyber threat landscape affecting the European offshore wind sector within the AENAON project. It identifies the main cyber threats, exposed dependencies and operational weaknesses that may affect offshore wind farms, and why these risks matter for Europe's energy security and electricity system resilience. The analysis is timely: wind energy supplied 20% of EU electricity generation in 2025, while offshore wind is becoming a strategic energy security pillar through growing installed capacity, cross-border interconnection and reliance on digitally enabled infrastructure whose disruption could have consequences beyond individual operators.

The report combines evidence from publicly reported incidents, open-source intelligence on exposed digital assets, analysis of offshore wind digital architecture and stakeholder input collected through the AENAON questionnaire. Together, these sources establish a common baseline for understanding the sector's current exposure and for informing the requirements, cyber range scenarios and managed security services developed in AENAON. They show that offshore wind cyber exposure is not limited to turbine control systems. The most critical dependencies sit across the operational ecosystem that enables offshore wind farms to be monitored and maintained, including SCADA environments, remote access channels, OEM platforms, telecommunication links, cloud services, trader and TSO interfaces, maintenance providers and third-party support tools.

The report also establishes an initial reference offshore wind use case, based on the representative digital architecture, stakeholder interfaces and operational dependencies described in Section 2. This reference environment provides the common basis against which the subsequent threat, attack-surface, impact and preparedness analyses are interpreted. Based on this evidence, the report derives an initial set of preparedness-support, cyber-range/training and regulatory-support requirements, mapped at AENAON service-area level and intended for subsequent stakeholder validation and refinement.

Remote access, third-party connectivity, OEM dependency, legacy OT and limited asset visibility represent the most significant perceived and observed exposure. Questionnaire responses strongly reinforce this with SCADA, communications infrastructure and remote-access systems being repeatedly identified as critical, while OEM vendors and ICT supply chain actors were highlighted as core external dependencies. The publicly reported incidents affecting wind or adjacent energy organisations also point in the same direction.

The threat analysis identifies ransomware as the most frequently observed threat across the reported incidents. Cybercrime actors represent the most consistently active and highest-likelihood adversary category, through ransomware, data theft and double-extortion activity. State-nexus actors are assessed as the lowest-frequency but highest-consequence category, and the highest-impact scenarios are accordingly associated with state-nexus actors, wiper malware, OT/ICS-targeted attacks and supply chain compromise, affecting trusted control environments, communications, restoration capability and the integrity of operational data. Hacktivists, hybrid and information

operations actors are reported less frequently in offshore wind incidents, but remain relevant because of the sector's high political visibility, maritime footprint and strategic importance for European energy policy.

The impact analysis shows that cyber incidents may affect offshore wind operations in many ways. Direct revenue loss can arise from unavailable generation, but consequences also include degraded grid coordination, loss of trusted telemetry, delayed fault diagnosis, impaired maintenance logistics, safety and environmental exposure, reputational harm, regulatory obligations and increased recovery costs. For large offshore portfolios, even short disruptions can place substantial gross revenue at risk. More importantly, a sudden loss of generation may create wider grid-stability concerns. Offshore-specific constraints such as weather conditions, vessel access or OEM support can further extend recovery timelines.

Over the next 12 to 24 months, the threat landscape is expected to be shaped by the convergence of ransomware, destructive malware, remote-access compromise, supplier disruption, exploitation of exposed infrastructure and AI-enabled improvements to existing attack methods. Offshore wind cybersecurity must be treated as an operational resilience priority rather than only as a technical security issue.

2. List of figures

Figure 1: Methodology overview — three complementary data collection strands and their integration.19

Figure 2: European fossil fuel imports dependency / Source: WindEurope (2025)24

Figure 3: Reference digital architecture of the AENAON offshore wind use case29

Figure 4: Threat category in reported incidents37

Figure 5: Affected asset layer in reported incidents38

Figure 6: The collapse of time-to-exploit: interval between public disclosure of a vulnerability and first confirmed exploitation in the wild, 2018–2026 / Source: Zero Day Clock (2026).54

Figure 7: Adversary Comparison for Offshore Wind64

3. List of tables

Table 1: Reported incidents35

Table 2: Threat category of the observed incidents and identified primary MITRE technique 42

Table 3: Financial impact from OWF operational disruption71

Table 4: Coverage categories103

Table 5: Capability areas used in the mapping103

Table 6: Baseline legal obligations under NIS2 and CRA104

4. Acronyms & Abbreviations

5G	Fifth-generation mobile network
AENAON	Ex-Ante cybersecurity Federated Digital twin-based Cyber Range and managed security services for offshore wind farms
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AVR	Automatic Voltage Regulator
BMWE	Federal Ministry of Economic Affairs and Energy, Germany
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CETaS	Centre for Emerging Technology and Security
CHP	Combined Heat and Power
CIRCL	Computer Incident Response Center Luxembourg
CISA	Cybersecurity and Infrastructure Security Agency
CMS	Condition Monitoring System
CRA	Cyber Resilience Act
CSIRT	Computer Security Incident Response Team
CSV	Comma-Separated Values
CTL	Cybersecurity Threat Landscape
CTV	Crew Transfer Vessel
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration

DDoS	Distributed Denial-of-Service
DMS	Distribution Management System
DMZ	Demilitarised Zone
DNP3	Distributed Network Protocol 3
DOE	United States Department of Energy
DoS	Denial-of-Service
DP	Dynamic Positioning
DSO	Distribution System Operator
E3C	Energy Emergencies Executive Committee
EMS	Energy Management System
ENISA	European Union Agency for Cybersecurity
ESO	Electricity System Operator
EU	European Union
EUR	Euro
FAT	Factory Acceptance Testing
FBI	Federal Bureau of Investigation
FiP	Feed-in Premium
FIPS	Federal Information Processing Standards
FiT	Feed-in Tariff
FSB	Federal Security Service of the Russian Federation
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
GW	Gigawatt
HAT	Harbour Acceptance Testing

HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICRTP	Interactive Cyber Range Training Programme
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IP	Internet Protocol
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Centre
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
JSON	JavaScript Object Notation
KA-SAT	Viasat Ka-band satellite communications network
LFDD	Low Frequency Demand Disconnection
MFT	Managed File Transfer
MITRE	The MITRE Corporation
MW	Megawatt
MWh	Megawatt-hour
NASK	Research and Academic Computer Network, Poland
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre, United Kingdom

NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSEC	North Sea Energy Cooperation
NVD	National Vulnerability Database
NVR	Network Video Recorder
ODBC	Open Database Connectivity
OEM	Original Equipment Manufacturer
ONVIF	Open Network Video Interface Forum
OPC	Open Platform Communications
OPR	Owner's Peripheral Router/Firewall
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
OWF	Offshore Wind Farm
PC	Personal Computer
PLC	Programmable Logic Controller
PoC	Point of Connection
PPA	Power Purchase Agreement
PRC	People's Republic of China
PV	Photovoltaic
RaaS	Ransomware-as-a-Service
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RTU	Remote Terminal Unit
SANS	SANS Institute
SBOM	Software Bill of Materials



SCADA	Supervisory Control and Data Acquisition
SD-WAN	Software-Defined Wide Area Network
SFTP	SSH File Transfer Protocol
SIS	Safety Instrumented System
SMTP	Simple Mail Transfer Protocol
SOV	Service Operation Vessel
SQL	Structured Query Language
SSH	Secure Shell
STL	Sectorial Threat Landscape
TCA	Transient Cyber Asset
TCP	Transmission Control Protocol
TDIR	Threat Detection, Investigation and Response
TSO	Transmission System Operator
TWh	Terawatt-hour
UK	United Kingdom
UPS	Uninterruptible Power Supply
US	United States
USD	United States Dollar
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network
VSA	Virtual System Administrator
WP	Work Package
xBOM	Extended Bill of Materials
XML	Extensible Markup Language



5. Introduction

Scope & Sector Definition

Wind energy is already a central component of Europe's electricity system and a key enabler of the energy transition. In 2025, wind supplied 20% of EU electricity generation, with offshore wind representing a growing share of new capacity buildout in a highly interconnected system (WindEurope, 2026). Offshore wind is therefore not only a renewable generation technology, but also a strategic infrastructure sector whose availability and resilience matter for European energy security and industrial competitiveness.

The sector's relevance is reinforced by European and regional policy commitments, including the European Green Deal (European Commission, 2019), the EU Strategy on Offshore Renewable Energy (European Commission, 2020), North Sea countries' cooperation processes (BMWE, 2026) and national offshore wind targets, which continue to drive deployment at scale. As the installed offshore wind base expands and becomes more interconnected, cyber risk must be assessed in relation to operational continuity, trusted data exchange, remote maintenance, grid coordination and recovery capability.

For the purposes of this report, the offshore wind sector is understood as the operational and digital ecosystem that enables offshore wind farms to generate, transmit, monitor and maintain electricity production. This includes turbines, offshore and onshore substations, SCADA and control systems, communications infrastructure, remote access channels, OEM platforms, maintenance providers, cloud services, condition monitoring systems, trader interfaces and transmission system operator interfaces. The scope therefore extends beyond individual turbine control systems to the wider network of technical, organisational and supply-chain dependencies that support offshore wind operations.

In addition to defining the sectoral scope of the threat landscape, D2.1 establishes an initial reference offshore wind use case for AENAON. The use case is represented through a generic offshore wind farm operating environment rather than a site-specific deployment and covers the principal assets, network segments, stakeholders, operational interfaces and dependencies relevant to cyber preparedness. The reference environment is further analysed through the threat scenarios, attack pathways and potential consequences presented in Sections 3-8.

In parallel, D2.1 consolidates an initial requirements baseline derived from the sector context, stakeholder input, threat landscape, regulatory analysis and identified preparedness gaps. The baseline covers preparedness-support services, cyber-range and training needs, and regulatory-support requirements. These initial requirements are presented in Appendix C and are intended to support subsequent refinement through T2.2 and T2.3 towards the M10 use-case and requirements specification milestone.

Reporting period

The reporting period runs from January 2021 to June 2026. The outlook presented in Section 8 extends 12 to 24 months beyond it.

The three evidence streams cover different windows within that period. The incident record reviewed in Section 3.1 is concentrated from 2021 to 2025, the years in which the wind-sector and adjacent energy incidents most relevant to offshore wind were publicly reported. A small number of earlier incidents, dating from 2015 to 2020, are retained despite falling outside the reporting period, because they remain the clearest public examples of OT and ICS-targeted attack techniques and of SCADA-focused espionage against energy infrastructure, and no comparable later cases have been disclosed.

The OSINT scanning was carried out in March 2026 and reflects internet-facing exposure as it stood at that point; as noted in Section 1.5 and Appendix A, it is a single collection window rather than a continuous measure. The questionnaire was fielded between May and June 2026 across its two deliveries.

Where developments after June 2026 are referenced, most notably in the discussion of AI-enabled threats in Section 4.8, they are drawn from external sources rather than from the project's own collection and are identified as such in the text.

Target audience

This report is written for three audiences, following the strategic, tactical and operational segmentation of the ENISA Cyber Threat Landscape methodology.

Strategy level readers: policymakers, regulators, boards and investors. These are served by Sections 2, 3, 7 and 8, which establish the sector's criticality, the observed threat picture, the consequences of disruption and the outlook over the next 12 to 24 months, together with the strategic recommendations in Section 9.1.

Tactical level readers: security managers, risk owners and IT/OT leads within operators, OEMs and service providers. These are served by Sections 4, 5 and 6, which characterise the primary threats, the adversaries behind them, and the attack surface created by the sector's supply chain and remote access dependencies.

Operational level readers: SOC analysts, incident responders and engineering teams. These are served by Sections 6.3, 9.2 and 9.3, and by the methodology annex in Appendix A, which sets out how the evidence was gathered and what it does and does not support.

It should be highlighted that this report is unclassified and intended for open circulation among AENAON partners, sector stakeholders and the wider European offshore wind and energy security community.

Intelligence Requirements & Key Questions



The analysis was directed by six intelligence requirements, each expressed as a question the report sets out to answer. They shaped the collection described in Section 1.5 and the structure of the chapters that follow.

1. **Criticality**. Why does the cyber security of offshore wind matter beyond the operators themselves, and what makes it a European energy security concern rather than a purely commercial one? Addressed in Section 2.
2. **Observed and perceived threat activity**. Which cyber incidents have affected wind energy and adjacent energy organisations, what threat types do they represent, and how does that record compare with what practitioners in the sector perceive as most severe? Addressed in Sections 3 and 4.
3. **Adversaries**. Which threat actor categories are relevant to offshore wind, what are their motivations and capabilities, and which of them present the highest-impact risk? Addressed in Section 5.
4. **Attack surface and dependencies**. Where is the sector exposed, particularly through remote access, OEM relationships, third-party platforms, legacy operational technology and cross-border interconnection? Addressed in Section 6.
5. **Impact**. What operational, grid-level, safety, environmental, economic and reputational consequences follow from a successful attack, and how are they amplified by offshore-specific constraints? Addressed in Section 7.
6. **Outlook and response**. How is the threat landscape expected to evolve over the next 12 to 24 months, and what should operators, suppliers and policymakers do within that window? Addressed in Sections 8 and 9.

Methodology Overview

The methodology draws on three complementary data collection approaches.

The first is desk research, comprising a review of open sources, scientific publications and grey literature to identify and characterise all notable past cyber security incidents affecting wind farms, establishing the historical baseline against which current exposure is assessed.

The second is open-source intelligence (OSINT) scanning of internet-facing assets, which captures a snapshot of the devices currently exposed to the internet, providing an externally visible picture of wind energy assets, their associated vulnerabilities, and the supply chain risks they imply. This approach is akin to what an attacker may do during the Reconnaissance phase of an attack.

The third is a structured questionnaire designed to capture the operator and stakeholder perspective: how organisations perceive cyber threats, where they see gaps in preparedness, and their appetite for collaborative initiatives. The questionnaire was fielded through two separate deliveries. The first was conducted through the European Defence Agency's Consultation Forum for Sustainable Energy in the Defence and Security Sector

(CF SEDSS), in which AENAON partners participated; capturing perceptions of cyber security in the defence context was considered critical given the wider geopolitical situation, and provides a holistic view of not only the current landscape but also its likely trajectory over the short and long term. The second was delivered online to WindEurope members and stakeholders, principally wind farm operators.

Together, these three methods offer a more complete view than any could provide alone. The desk research establishes what has already happened to wind farms and how attacks against them have been executed. The OSINT scanning reveals what was found to be publicly exposed at the time of the research, and thus potentially exploitable from the outside. The questionnaire surfaces the human, organisational, and operational dimensions that technical scanning cannot reach. The two questionnaire deliveries together support the composition of a threat landscape while focusing attention on the most imminent gaps. By combining historical incident analysis and passive external reconnaissance with direct operator and stakeholder insight, the methodology is designed to bridge the gap between observed exposure and lived experience in the sector. Figure 1 summarises the three collection strands and how they are integrated.

1 · DESK RESEARCH **Historical incident review**	**2 · OSINT SCAN** **Current exposure snapshot**	**3 · QUESTIONNAIRE** **Practitioner perception**
Systematic review of open sources, scientific publications and grey literature covering all notable past cyber security incidents affecting wind farms and their operators.	Targeted queries against Internet-facing wind energy assets — turbine OEM systems, ICS protocols, SCADA, management platforms and remote access — enriched with CVE severity data from CIRCL and NVD.	Two deliveries: (a) EDA Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) — defence and geopolitical perspective; (b) online survey of WindEurope members and stakeholders — wind farm operators.
Output: historical baseline — which threat types have actually materialised in the sector.	Output: externally visible attack surface, vulnerability status and supply chain exposure.	Output: perceived threats, preparedness and capability gaps, appetite for collaboration.

▼ ▼ ▼

INTEGRATED ANALYSIS — triangulation of the historical record, current external exposure and practitioner perception, producing the AENAON offshore wind sectorial threat landscape and the imminent capability gaps it reveals.

Figure 1: Methodology overview — three complementary data collection strands and their integration.

Open-source intelligence

Wind energy infrastructure is increasingly networked and internet-connected, creating potential exposure to cyber threats. The goal of this analysis was to map the publicly accessible attack surface associated with wind energy assets at a given point in time and to assess their vulnerability status. The exercise is deliberately a snapshot: it records which devices and services were exposed during the collection window, and the technologies, vendors and platforms visible in that exposure also indicate where supply chain risk concentrates. By identifying which devices and services are visible on the open internet, and cross-referencing these with known vulnerability databases, this work aims to provide a clearer picture of the cybersecurity risks facing the wind energy sector.

To this end, we identify Internet-facing assets associated with wind energy infrastructure using Shodan, a search engine that indexes publicly accessible devices and services connected to the internet.

A set of targeted search queries was constructed across several categories. These covered turbine Original Equipment Manufacturers (OEMs), industrial control system (ICS) protocols, SCADA software, management platforms, remote access services, and known-vulnerability indicators. The queries were executed against the Shodan Search API, and matching host banners were retrieved for each query.

The raw results contained a range of exposure data. This included IP addresses, open ports, software versions, and vulnerability identifiers already flagged by Shodan.

Common Vulnerabilities and Exposures (CVE) identifiers were then extracted from the results and enriched with severity metadata from two complementary sources. The first was the CIRCL CVE Database[1], operated by the Computer Incident Response Center Luxembourg (cicl.lu). The second was the U.S. National Vulnerability Database[2] (NVD), maintained by NIST. The NVD served as a backfill for older or less widely catalogued vulnerabilities where CIRCL data was incomplete. This two-source approach ensured broad coverage.

Enrichment included CVSS base scores and vectors, CWE classifications, and publication dates.

The entire pipeline was implemented as a single reproducible automation script, covering every stage, from query execution through to enrichment and export. Built-in caching and rate limiting were included to respect API usage policies.

The resulting dataset was exported as structured CSV and JSON files for subsequent statistical analysis and visualisation. Because it reflects a single collection window, the dataset should be read as an indicative snapshot rather than a continuous measure of

[1] https://www.circl.lu/services/cve-search/
[2] https://nvd.nist.gov/

exposure: hosts may appear or disappear as configurations, addressing and vendor deployments change.

Surveying Offshore Wind Industry

The questionnaire was developed as a primary data collection instrument to map the cybersecurity threat landscape across the offshore wind sector, targeting operators, asset managers, and operations and maintenance service providers, alongside defence and security stakeholders engaged in energy resilience. As set out above, it was fielded through two deliveries: the European Defence Agency's Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS), and an online delivery to WindEurope members and stakeholders. It was structured around three core objectives: characterising the current threat environment as experienced by practitioners, diagnosing where the sector is under-resourced or under-tested, and assessing appetite for collaborative initiatives such as open calls and joint exercises.

This design approach is consistent with structured threat landscape methodologies, such as the ENISA Cyber Threat Landscape (CTL) framework, which advocates sector-specific analysis, systematic data collection processes, and the production of actionable intelligence tailored to defined stakeholder audiences. Our design reflects three principles. First, sector specificity; generic cybersecurity surveys rarely capture the operational realities of offshore wind, where IT/OT convergence, remote operating conditions, complex supply chains, and cross-border regulatory exposure create a distinct threat surface. Second, proportionality; given respondent sensitivity around incident disclosure and architectural detail, the questionnaire uses banded response options, conditional branching, and optional open-text fields to minimise disclosure risk without sacrificing analytical value. Third, actionability; each section was mapped to a defined analytical output from the outset, rather than constructed opportunistically.

The questionnaire moves through six thematic sections: organisational context (scale, geography, operating model, OT dependency), digital and operational exposure (remote access use, third-party connectivity, legacy systems, asset criticality), threat perception, cybersecurity preparedness and capability gaps, sector-level vulnerability, and finally appetite for participation in AENAON open calls.

Twenty-seven valid responses were received across the two deliveries, spanning seven organisational categories: wind farm operators (n = 7), defence organisations (n = 8), energy utility or grid operators (n = 4), maintenance and O&M providers (n = 3), public authorities and regulators (n = 2), OEM manufacturers (n = 1), and two further respondents. For comparative analysis the sample was consolidated into three analytically distinct groups reflecting both the project's focus and the operational divergences observed in the data: an Energy group (wind farm operators and energy utilities, n = 11), a Defence group (n = 8), and an Others group comprising sector-adjacent organisations (n = 8). Item-level completion varied across the instrument, and one question was excluded from analysis owing to a high blank-response rate.

Analysis proceeded in three phases. The first established overall response distributions across the full sample, testing whether observed proportions and associations differ from chance. The second applied a dedicated ranking analysis to the threat and entry-point questions, combining composite scoring, inter-rater agreement measures, and hierarchical clustering to identify tiers of concern. The third compared groups pairwise, both as Energy against non-energy respondents and across the three-group structure, with correction for multiple comparisons and effect sizes reported throughout. Given the sample size, all findings are treated as exploratory and hypothesis-generating rather than confirmatory. The threat perception findings are discussed in Section 3.2, alongside the tracked incident data; the full statistical treatment is reported separately.

6. Offshore Wind Use Case Foundations & Sector Context

This section establishes the operational and sectoral foundations of the AENAON reference offshore wind use case. It describes the strategic and regulatory context in which the use case operates and defines a representative offshore wind digital environment, including the main asset groups, network segments, external stakeholders, communications pathways and operational dependencies. The reference environment is intentionally generic so that it can support AENAON preparedness, cyber-range and training activities across different offshore wind deployments without representing the configuration of a specific operator. Sections 3-8 subsequently analyse the threats, attack pathways, dependencies and consequences applicable to this reference environment.

Role of Wind Energy in EU Energy Security

The cyber and physical resilience of energy infrastructure is no longer optional but an integral part of Europe's energy security. The continuous energy crises of recent years, with Russia's invasion in Ukraine and, more recently, the closure of the Strait of Hormuz, have repeatedly exposed Europe's dependence on imported fossil fuels. Each crisis has reinforced the conclusion that energy security is not simply a question of how much energy is available but also a question of where it originates. The EU's policy response, set out in the REPowerEU Plan, explicitly links the accelerated deployment of renewable generation to reducing dependence on imported Russian fossil fuels (European Commission, 2022).

An economy powered by cheap, homegrown renewables is less exposed than one dependent on unreliable, volatile and costly fossil fuel imports. This is further reinforced by WindEurope's energy systems cost study (WindEurope, 2025a). The study shows that an energy system driven by renewables and high electrification reduces fossil fuel dependency from 71% in 2030 to 22% in 2050. On contrary, a Slow Transition scenario leaves Europe dependent on fossil fuel imports with a modest reduction to 54% (Figure 2).

Wind energy is already central to reducing this dependency. In 2025, it accounted for 20% of Europe's electricity generation (WindEurope, 2026), and it is a mature and scalable technology built largely on European manufacturing capacity, with a great potential to further displace fossil fuel imports. The recent Hamburg pledges (BMWE, 2026) about offshore wind reinforced the trust and importance European governments put into the sector. At EU level, these commitments are underpinned by the European Wind Power Action Plan, which sets out measures on permitting, grid access, supply-chain resilience and sector competitiveness (European Commission, 2023).

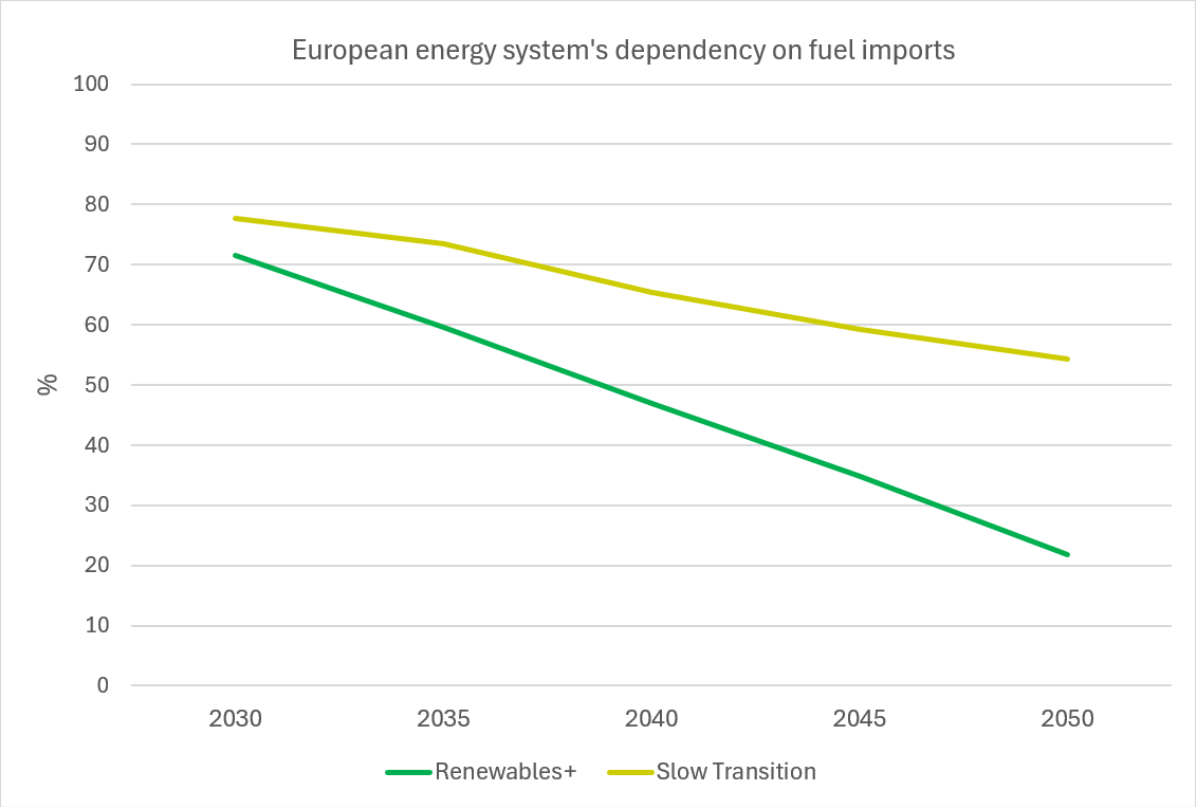

Figure 2: European fossil fuel imports dependency / Source: WindEurope (2025)

Regulatory Landscape

Offshore wind farms operate within an increasingly complex cybersecurity and resilience regulatory environment. As critical energy infrastructures, they rely on interconnected digital systems, operational technologies, remote communications, third-party service providers and cross-border operational dependencies that collectively increase both cybersecurity exposure and compliance obligations. Consequently, cybersecurity governance within offshore wind farm environments extends beyond conventional information security practices and must address operational resilience, supply-chain security, cyber-physical risk management and incident preparedness.

Within the European Union, the framework most relevant to offshore wind farm cybersecurity is primarily shaped by the NIS2 Directive and the Cyber Resilience Act (CRA). While these instruments address different dimensions of cybersecurity governance, they are complementary in practice: NIS2 focuses on the responsibilities of operators and critical entities, whereas the CRA focuses on the cybersecurity characteristics of products with digital elements deployed within operational environments. Additional obligations may arise from other legal frameworks, including the GDPR and the AI Act, depending on the characteristics of the affected systems and the nature of the incident.

The Network and Information Security (NIS2) Directive

The NIS2 Directive (European Union, 2022), which Member States were required to transpose by October 2024, establishes updated cybersecurity obligations for essential and important entities across the EU, including those operating critical energy infrastructure. Its objective is to strengthen resilience across the Union by introducing common requirements for governance, cybersecurity risk management, incident reporting, operational continuity and supply-chain security.

Wind energy producers, both offshore and onshore, fall within the Directive's energy sector scope as electricity producers listed in Annex I. Whether a given operator is treated as an essential or an important entity is not determined by generation capacity alone: it depends on the applicable Annex I entity type, on the Article 3 size criteria, and on designation routes under Article 2(2) that can apply irrespective of size, as well as on national transposition choices. As a general rule, operators exceeding the ceilings for medium-sized enterprises are treated as essential entities and those meeting the medium-sized criteria as important entities, but classification should be confirmed case by case against the applicable national implementing law. The Directive requires organisations to implement risk-based security measures across both information technology (IT) and operational technology (OT) environments, with particular focus on systems such as SCADA. It mandates a phased incident reporting regime, with an early warning within 24 hours of awareness, a full incident notification within 72 hours and a final report within one month, regular audits by competent authorities, and imposes heavy penalties for non-compliance, for essential entities, at least up to €10 million or 2% of total worldwide annual turnover, whichever is higher. The Directive places emphasis on cybersecurity risk management and governance; incident handling and reporting procedures; business continuity and disaster recovery planning; supply-chain and third-party security management; cyber hygiene and access control; monitoring, detection and effectiveness assessment; and management accountability and organisational oversight.

In practice, this means operators must actively secure their control systems, turbine networks and communication channels. Supply-chain security has a particular focus: operators must ensure that vendors and service providers meet cybersecurity standards, which extends cybersecurity expectations to wind OEMs through contractual and procurement requirements. Additionally, OEMs may fall within the scope of the Directive as important entities in their capacity as manufacturers. OEMs must therefore build cybersecurity into their products and operations, ensuring that hardware and software components used in turbines and control centres are resilient against threats.

The offshore context introduces additional complexity. Offshore wind farms operate through geographically distributed assets, remote communications infrastructure and specialised maintenance arrangements, creating operational dependencies that can amplify the impact of cybersecurity incidents. Compliance therefore requires not only technical controls but also resilient organisational processes capable of supporting operational continuity under degraded conditions.

While these obligations are significant, alignment with NIS2 offers strategic advantages. Operators and OEMs that demonstrate robust cybersecurity postures can improve their standing with regulators, investors and customers, gaining a competitive edge in a market increasingly sensitive to risk management and operational resilience.

The EU Cyber Resilience Act (CRA)

While NIS2 focuses on organisations and infrastructure, the Cyber Resilience Act (European Union, 2024a), entered into force in 2024 with manufacturers' vulnerability and incident reporting obligations apply from September 2026, and the main obligations from December 2027, targets the products themselves. It introduces cybersecurity requirements for all products with digital elements placed on the EU market, subject to limited exclusions for sectorally regulated products, aiming to ensure security from design through the entire product lifecycle by promoting secure-by-design principles, vulnerability management, security maintenance and transparency obligations.

The CRA's relevance for offshore wind stems from the extensive use of digital technologies across operational infrastructure, including industrial control systems, monitoring platforms, communication equipment, remote-access solutions and vendor-provided software. The security posture of these technologies directly influences the resilience of offshore operations and the effectiveness of operator-side measures.

Under the CRA, OEMs developing turbines, controllers, sensors and related software must integrate cybersecurity from the earliest design stages. Risk assessments must be conducted, vulnerabilities managed proactively after products are sold, and regular security updates provided to address emerging threats. Products must ship with secure default settings, and in higher-risk categories, conformity assessment procedures or third-party certifications will be required before market placement. Accordingly, emphasis is placed on secure-by-design and secure-by-default principles; vulnerability identification and remediation; security updates and lifecycle maintenance; authentication and access control; logging, monitoring and observability; and product-security transparency and software assurance.

For the wind sector, this shift is profound. OEMs must embed secure development lifecycles into their engineering processes and maintain active monitoring and patching programmes for deployed equipment, making security a core requirement rather than a feature. Operators benefit indirectly, procuring products that meet a higher cybersecurity baseline and thereby reducing operational risk. Although many CRA obligations apply primarily to manufacturers, importers and distributors, the regulation provides an important reference framework for evaluating the security characteristics of technologies deployed within offshore operational environments.

Meeting CRA requirements demands significant investment, especially for retrofitting security into legacy product lines, but it is also an opportunity: demonstrably secure products will gain a competitive advantage, reassuring customers, investors and insurers,

and CRA compliance will likely become a prerequisite for accessing many European energy markets over time.

General Data Protection Regulation

While NIS2 and the CRA constitute the primary cybersecurity-specific frameworks relevant to offshore wind farm environments, cybersecurity incidents may also trigger obligations arising under the General Data Protection Regulation (European Union, 2016). This is particularly relevant where incidents involve personal data breaches, credential compromise, unauthorised access to personnel information or data exfiltration activities associated with ransomware and double-extortion attacks.

In such situations, organisations may be required to coordinate cybersecurity incident response activities with personal data breach assessment, notification and remediation procedures. Consequently, effective cybersecurity governance within offshore environments requires awareness of the interaction between cybersecurity obligations and data protection responsibilities, particularly when cyber incidents affect identifiable individuals or employee-related information.

EU AI Act

The AI Act may become relevant where artificial intelligence systems are integrated into cybersecurity monitoring, anomaly detection, threat intelligence analysis, risk assessment or operational decision-support functions (European Union, 2024b; ENISA, 2023). As offshore wind farm operators increasingly adopt advanced analytics and AI-enabled technologies, regulatory obligations relating to trustworthy and accountable AI systems may become increasingly significant.

The AI Act follows a risk-based regulatory approach and introduces obligations relating to transparency, human oversight, accountability and risk management. While the specific applicability of these obligations depends on the role and classification of the AI system concerned, the regulation establishes an important governance framework for organisations deploying AI-enabled capabilities within critical infrastructure environments.

EU Data Act

The Data Act, applicable since September 2025, governs access to and sharing of data generated by connected products and related services, and is directly relevant to offshore wind environments given the volume of operational data produced by turbines, sensors and monitoring systems (European Union, 2023). The Regulation grants users of connected products, including wind farm operators, rights to access the data their assets generate and to share it with third parties, while imposing corresponding obligations on data holders, typically OEMs and service providers, to make such data available under fair, reasonable and non-discriminatory conditions.

These provisions are particularly significant for data-intensive applications such as digital twins, predictive maintenance and performance optimisation, which depend on structured data flows across the OEM–operator–service provider chain. From a cybersecurity

perspective, the Data Act also introduces requirements on safeguarding shared data, protecting trade secrets in data-sharing arrangements, facilitating switching between data processing services, and preventing unlawful international governmental access to non-personal data held in the EU. Effective governance of offshore wind data therefore requires reconciling data-sharing obligations with security, confidentiality and access-control measures, an interaction that becomes more acute as digitalisation of offshore operations deepens.

An Evolving Regulatory Landscape

The regulatory framework described above should not be regarded as static. In January 2026, the European Commission presented a legislative package revising the EU cybersecurity acquis, including a proposal for a revised Cybersecurity Act (European Union, 2019; European Commission, 2026) and measures to simplify and streamline the implementation of NIS2. Among the most consequential elements for the energy sector are the proposed provisions on ICT supply-chain security, which would establish mechanisms for assessing and, where necessary, restricting the use of high-risk suppliers for critical ICT functionalities within essential infrastructure. For offshore wind, a sector characterised by long asset lifetimes, complex international supply chains and deep dependence on vendor-provided control systems, SCADA platforms and remote-access solutions, such measures could significantly reshape procurement, product qualification and vendor management practices. In parallel, cybersecurity considerations are increasingly being embedded in adjacent policy instruments, including resilience and pre-qualification criteria in national offshore wind auction frameworks under the Net-Zero Industry Act, and sector-specific initiatives on cybersecurity for renewable generation assets. Organisations operating in offshore wind environments should therefore treat regulatory monitoring as an integral component of cybersecurity governance, anticipating that compliance obligations will continue to expand in scope, granularity and enforcement intensity over the coming years.

Reference Digital Architecture of the Offshore Wind Use Case

General Description

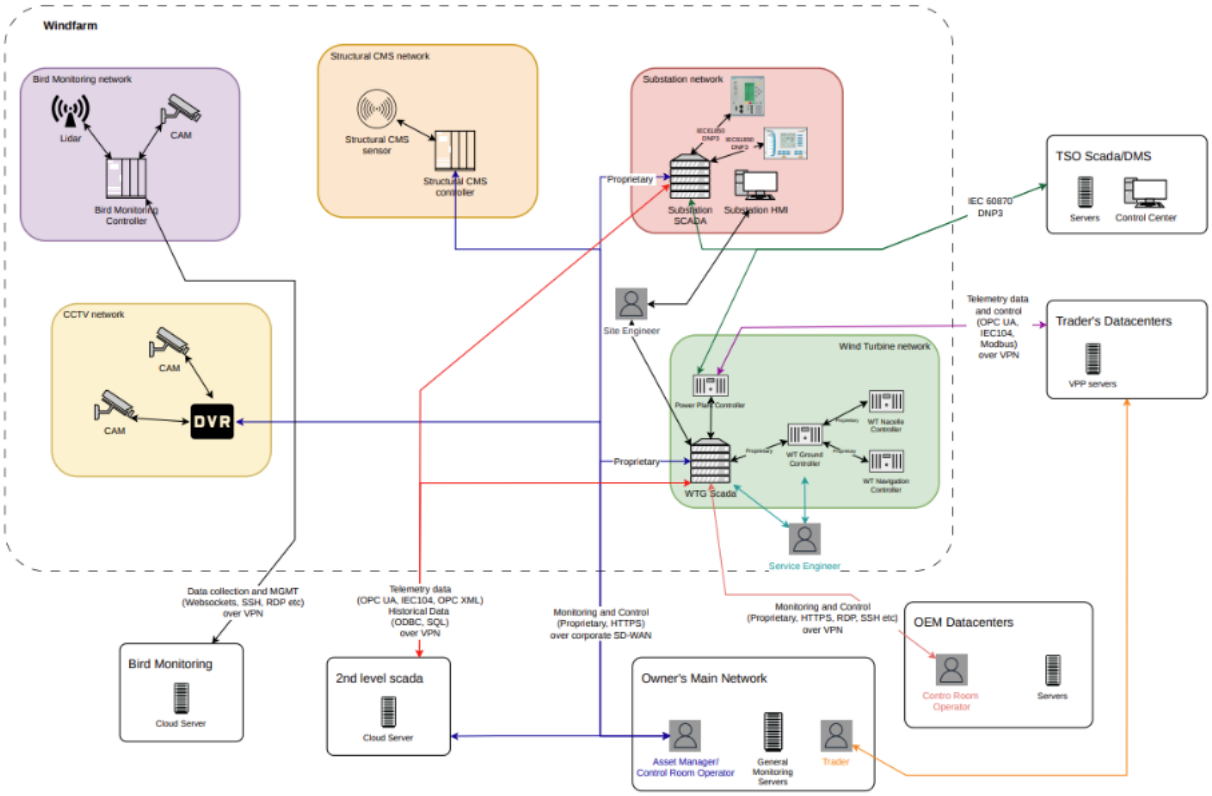

Figure 3: Reference digital architecture of the AENAON offshore wind use case

The reference digital architecture of the AENAON offshore wind use case is presented in Figure 3. An offshore wind farm network typically consists of the following network segments:

- The wind turbine Original Equipment Manufacturer network
- The substation protection network
- Auxiliary equipment networks, including the CCTV/alarm network, the bird detection system network, and the structural condition monitoring system (CMS) network

The wind farm owner/operator ensures that internet access is provided to the wind farm networks through an Owner's Peripheral Router/Firewall (OPR). Redundant internet connections are typically used (e.g. direct internet access, satellite, and 5G) to achieve the highest possible availability. Internet access is primarily used to interconnect local wind farm systems with various peripheral stakeholders. The most important stakeholders are:

- The owner/operator headquarters network for monitoring, control, remote administration, and reporting
- The OEM central network for monitoring and administering wind turbine OEM devices, especially in cases where full-scope agreements are in place
- The energy trader's headquarters for telemetry exchange and wind farm power output regulation according to market conditions
- The transmission system operator (TSO) network for telemetry exchange and wind farm power output regulation according to grid conditions
- Cloud servers for auxiliary devices, such as the bird detection system, which collect sensor data for further analysis and categorization
- Cloud servers as a second-level SCADA solution, a vendor-agnostic asset performance monitoring tool that collects real-time and historical data from the wind turbine OEM SCADA and the substation SCADA and provides centralized monitoring, analysis, and reporting.

Network segments

Wind Turbine OEM Network

The wind turbine OEM network consists of wind turbine controllers, such as Programmable Logic Controllers (PLC), HMIs, sensor devices, Power Plant Controllers (PLCs or server-based systems), and the main wind turbine SCADA server (typically a local Windows or Linux server). Internal data exchange depends on the OEM but mainly uses proprietary or standard industrial communication protocols. Administrative access to these devices is typically provided through protocols such as HTTP, HTTPS, and SSH. The historian database within the SCADA server is usually an SQL database.

The wind turbine OEM network is usually based on an industrial Ethernet/fiber-optic closed-loop architecture that uses spanning tree protocols to ensure high availability. The network is typically segmented into multiple VLANs and configured by the OEM during wind farm commissioning. The entire wind turbine network is protected by an OEM firewall, which is responsible for the outbound Virtual Private Network (VPN) connection to the OEM headquarters and for enforcing strict firewall rules toward the wind farm peripheral network.

When a full-scope agreement with the OEM is in place, the owner/operator may be granted access to SCADA resources either through a VPN profile that allows access to specific application ports for the proprietary SCADA client, the historian database, and an industrial protocol such as OPC for telemetry and control, or through a Demilitarized Zone Network (DMZ) interface with similar access. In this case, the OEM remains the network administrator for this segment.

In rare cases, the wind turbine OEM network may be decommissioned by the OEM, allowing the owner/operator to assume the role of network administrator and manage the network

devices independently. This is uncommon, as the OEM can no longer support or troubleshoot issues on the SCADA server or network devices and no longer provides remote 24/7 monitoring, which is typically included in full-scope agreements.

Substation Protection Network

The substation protection network is an industrial Ethernet/fiber-optic network that primarily uses substation protocols such as IEC 61850, DNP3, or similar. This network includes protection relays, bay control units, AVRs, RTUs, PLCs, and power measurement devices that exchange signals and events. General signals or information from peripheral devices are typically collected through standard industrial protocols such as Modbus TCP. A substation SCADA server gathers signals and events from the various substation devices and provides an HMI for real-time monitoring and control. At the same time, the substation SCADA maintains a historian database of signals and events for reporting purposes.

When substation signals and events must be transferred outside the perimeter of the local substation SCADA network, gateway devices are typically used (e.g., IEC 61850 or DNP3 to IEC 60870-5-104 or OPC UA).

The substation network is usually segmented in recent installations, creating a distinction between protection devices, auxiliary signal devices, and switching device management. The network administrator is typically the owner/operator, and the gateway is usually the Owner's Peripheral Router/Firewall (OPR).

CCTV/ Alarm Network

The CCTV/alarm network is a simple Ethernet/fiber-optic network segment in which all physical security related devices are interconnected. This network typically consists of IP cameras, video recording devices, and alarm system controllers and gateways. For video recording, the NVR collects video streams using either proprietary video streaming and camera control protocols or the open ONVIF standard. The same protocols are also used for remote streaming, playback, and equipment control. The network administrator is usually the owner/operator, and the gateway is typically the Owner's Peripheral Router/Firewall (OPR).

Bird Detection System Network

The bird detection system network depends heavily on the vendor specification. In general, it is an Ethernet/fiber-optic network consisting of cameras, radars/sensors, sound emission systems, and local controllers or databases per wind turbine. Although the devices across different wind turbines are interconnected, they are designed to function independently and to stop the wind turbines in the event of bird detection. The controllers require internet access to upload collected data and events to a cloud platform for further bird-flight analysis and statistics. Stop commands to the local wind turbine controllers/PLCs are typically sent either through dry contacts (hardwired signals) or through standard industrial protocols such as Modbus TCP or Modbus RTU.

The network administrator is usually the owner/operator, and the gateway is typically the Owner's Peripheral Router/Firewall (OPR).

Peripheral Stakeholders

Owner/ Operator

The owner/operator requires access to most wind farm resources for monitoring, operation, historical analysis, and administration. Access can be provided through one of the following methods, each offering a different level of security.

Use of a local PC with a remote desktop access application: Owner/operator employees use a remote desktop application (such as TeamViewer or AnyDesk) to connect to a local server that provides access to the various network segments within the wind farm.

VPN connection to the Owner's Peripheral Router/Firewall (OPR): The owner/operator's employees use a VPN client to connect to the OPR firewall. This connection provides access to the various network segments within the wind farm. Different VPN profiles can be created for specific employee groups to enforce differentiated access levels.

Permanent site-to-site VPN (or SD-WAN solution) with a DMZ inside the owner/operator's headquarters: The owner/operator's employees have permanent access to wind farm resources when connected to their corporate network. User-based access control is centralized, and specific access levels can be provided for each employee group.

The owner/operator includes roles such as asset managers, control room operators, and IT support personnel. The most common protocols required by the owner/operator are:

- Access to the OEM SCADA through the official client (HTTPS, proprietary protocols)
- Remote access to the substation SCADA PC (RDP, VNC, etc.)
- Device monitoring (ICMP, SMTP, etc.)
- Historical data collection (SQL, ODBC, etc.)
- Administration of various devices (HTTP, HTTPS, SSH, RDP, VNC, etc.)
- Remote data retrieval from auxiliary devices such as bird detection system controllers and data loggers (FTP, SFTP, etc.)
- Video streaming and camera control protocols (proprietary, ONVIF, etc.)

Original Equipment Manufacturer (OEM)

The OEM is another crucial stakeholder, especially when a full-scope agreement is in place. The OEM usually has a permanent VPN connection initiated by the OEM router/firewall toward the OEM headquarters. It uses its own infrastructure for monitoring, reporting, and analysis of wind farm devices. The OEM administers and configures all devices within the wind turbine network and collects and uses data from the OEM SCADA. In practice, it uses

many of the same protocols as the owner/operator, but only for wind turbine network devices.

Trader

The trader typically requires restricted access primarily to the wind farm Power Plant Controller. Its objective is to collect telemetry data at the Point of Connection (PoC) and dispatch power regulation commands to the wind farm. For this purpose, it typically uses industrial protocols such as Modbus TCP, OPC UA, or IEC 60870-5-104. Access is most commonly provided through one of the following methods:

- A site-to-site VPN with the OPR or the OEM firewall
- A site-to-site VPN with the owner's headquarters in case an SD-WAN solution exists

In both cases, a dedicated VPN profile is typically provided to allow access only to the Power Plant Controller and the required industrial protocol ports. The trader usually operates a cloud-based platform that automatically dispatches active power setpoint commands based on market conditions and provides the owner/operator and the owner's renewable energy aggregator with cloud-based monitoring and reporting.

Transmission System Operator (TSO) or Utility Company

The TSO typically connects to the substation protection network through a substation-focused industrial protocol such as DNP3, IEC 60870-5-104, or IEC 60870-5-101, usually through a gateway or RTU device. The TSO may install an on-site network device to establish its own VPN connection toward its EMS/DMS or use a leased line provided by an ISP. Its objective is to collect telemetry data at the Point of Connection (PoC), switchgear statuses, and protection activation events, and to dispatch various power regulation commands to the wind farm.

Second-Level SCADA

The second-level SCADA is a vendor-agnostic asset performance monitoring tool that collects real-time and historical data from the wind turbine OEM SCADA and the substation SCADA and provides a cloud platform for monitoring, analysis, and reporting. It typically gains access to the wind farm systems in one of the following ways:

- A site-to-site VPN with the OPR or the OEM firewall
- A site-to-site VPN with the owner/operator's headquarters
- Installation of data collectors inside the owner/operator's network, either locally at the wind farm or at the owner/operator's headquarters, which only push data toward cloud servers

The most common protocols used by a second-level SCADA solution to collect data are:

- Industrial real-time protocols such as OPC UA, OPC XML DA, OPC DA, and Modbus TCP for communication with the OEM SCADA and the substation network gateway/RTU



- Database protocols for historical data, such as ODBC and SQL, for communication with the OEM SCADA or the substation SCADA

The second-level SCADA has an API implementation, which allows all other stakeholders to easily get access to the collected data.

AENAON Reference Offshore Wind Use Case

For the purposes of AENAON, the reference use case represents a generic operational offshore wind farm comprising the wind turbine and OEM-controlled environment, offshore and onshore substation and protection systems, owner/operator monitoring and administration functions, communications infrastructure, remote-access pathways, auxiliary systems and the external digital interfaces required for operation. These interfaces include, where applicable, OEM monitoring and maintenance services, trader and transmission system operator connections, second-level SCADA and cloud-based monitoring services, telecommunications providers and specialist third-party support.

The use-case boundary therefore extends beyond individual wind turbine controllers. It includes the digital and organisational dependencies required to maintain visibility, control, dispatch, maintenance, fault diagnosis and restoration. Particular dependencies include remote connectivity, privileged OEM and supplier access, communications services, operational telemetry, cloud or externally hosted platforms, software and firmware support, and specialist maintenance capability. Compromise or unavailability of these dependencies can affect offshore operations even where turbine-control systems themselves remain uncompromised.

The reference use case provides the common environment for the threat scenarios analysed in the remainder of this deliverable. These include enterprise and ransomware compromise affecting operational support functions; remote-access and credential compromise; supplier and third-party compromise; communications disruption and loss of operational visibility; destructive activity affecting OT-connected systems; and targeted OT/ICS scenarios capable of affecting monitoring, control, substations or turbine-related functions. The associated cyber-to-physical, operational, grid, safety and economic consequences are examined in Sections 4-7.

The use case should therefore be read together with the threat landscape rather than as a standalone architecture description. Section 3 provides the observed and stakeholder-perceived threat context; Sections 4 and 5 characterise the relevant threats and adversaries; Section 6 examines the principal attack-surface and dependency pathways; Section 7 assesses potential operational and systemic consequences; and Section 8 provides the short-term outlook. Together, these elements establish the threat-informed baseline against which AENAON preparedness and cyber-range activities can be developed.

This use-case definition constitutes the initial reference baseline captured in D2.1. It is expected to be further refined through the ongoing stakeholder requirements and use-case specification activities of WP2 towards the corresponding M10 milestone, without

changing the representative offshore wind context established here. The initial requirements derived from this use case and from the threat, stakeholder, regulatory and

7. Threat Landscape Overview

Summary of Observed Incidents

Given the limited number of publicly reported incidents affecting offshore wind farms, this section is built on broader energy-sector incidents to characterise the threat landscape. An incident was recorded where at least one of the following criteria applies:

- The incident directly affected a wind farm operator, turbine OEM or their OT environment;
- The incident affected a supplier, OEM or service provider similar to those in the offshore wind supply chain;
- The incident affected the wider energy and utility sector, where the targeted asset class or threat actor is representative of what offshore wind operators may face;
- The incident is linked to a threat known to target energy infrastructure, even when the asset is located outside EU.

Table 1: Reported incidents

id	Incident Title	Year	Threat Type	Asset Layer	Impact Type	EU Rel.	Country
I-01	Coordinated wiper attacks on Polish renewable and CHP sites	2025	Wiper	OT/ICS	**Operational Disruption**	**High**	PL
I-02	KA-SAT/Viasat spillover – Enercon wind-turbine connectivity	2022	Wiper	Satellite Communications	**Communications Blackout**	**High**	DE (EU-wide)
I-03	Deutsche Windtechnik cyberattack	2022	Ransomware	IT Corporate	**Operational Disruption**	**High**	DE
I-04	Nordex cyber-security incident	2022	Ransomware	IT Corporate	**Operational Disruption**	**High**	DE
I-05	sPower firewall denial-of-	2019	DDoS	Network Infrastructure	**Communications Blackout**	**Low**	US



id	Incident Title	Year	Threat Type	Asset Layer	Impact Type	EU Rel.	Country
	service at wind and solar assets						
I-06	Vestas ransomware and data breach	2021	Ransomware	IT Corporate	**Mixed**	**High**	DK
I-07	Hitachi Energy GoAnywhere third-party breach	2023	Supply Chain Compromise	Cloud/Third-party Platform	**Data Breach**	**High**	CH
I-08	Kaseya VSA supply-chain ransomware attack	2021	Supply Chain Compromise	Cloud/Third-party Platform	**Operational Disruption**	**Low**	Global
I-09	HSE Slovenia ransomware attack	2023	Ransomware	IT Corporate	**Operational Disruption**	**High**	SI
I-10	BVIEC ransomware attack	2024	Ransomware	IT Corporate	**Operational Disruption**	**Low**	VG
I-11	Electrica Group ransomware attack	2024	Ransomware	IT Corporate	**Operational Disruption**	**High**	RO
I-12	Halliburton cyberattack – operational disruption and data theft	2024	Data Breach	IT Corporate	**Mixed**	**Medium**	US
I-13	Cyprus critical-infrastructure DDoS wave (utilities, EKO Cyprus)	2024	DDoS	Network Infrastructure	**Operational Disruption**	**High**	CY
I-14	Svenska kraftnät	2025	Data Breach	Cloud/Third-party Platform	**Data Breach**	**High**	SE

id	Incident Title	Year	Threat Type	Asset Layer	Impact Type	EU Rel.	Country
	external file-transfer breach						
I-15	Ukrainian power-grid cyberattack (Kyivoblenergo)	2015	OT/ICS Targeted Attack	OT/ICS	**Operational Disruption**	**High**	UA
I-16	Azerbaijan SCADA-focused espionage campaign	2020	Credential Abuse	SCADA	**Data Breach**	**Low**	AZ
I-17	South China Sea offshore-energy espionage campaign	2022	Credential Abuse	IT Corporate	**Data Breach**	**Medium**	Multiple (AP)
I-18	TRITON/TRISIS attack on safety-instrumented systems	2017	OT/ICS Targeted Attack	OT/ICS	**Operational Disruption**	**Medium**	SA

Table 1 lists the 18 incidents reviewed. Six out of 18 reported incidents directly affected the wind energy sector while the rest are drawn from the broader energy sector or from outside the EU, as described in the criteria above.

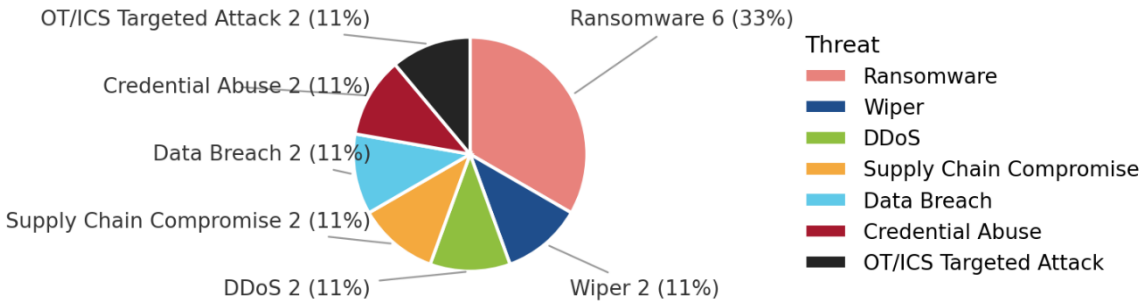

Figure 4: Threat category in reported incidents

As shown in Figure 4, ransomware accounts for the largest share with 6 out of 18 reported incidents. The remaining six categories are represented by 2 incidents each. This distribution reports what gets reported through publicly available data rather than the underlying risk distribution.

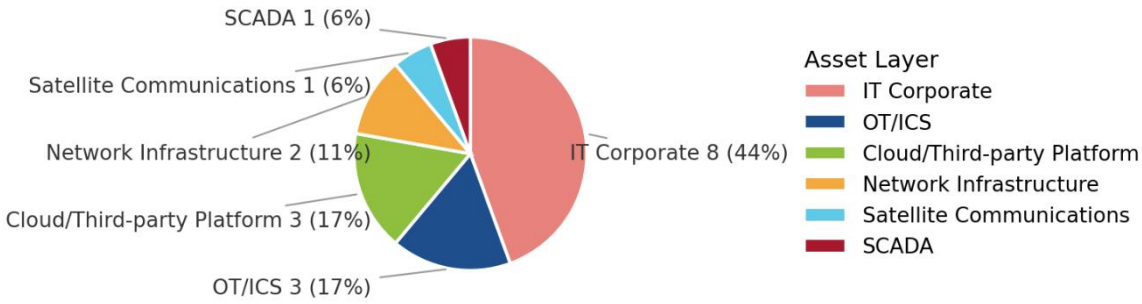

Figure 5: Affected asset layer in reported incidents

As shown in Figure 5, IT corporate systems are the most frequently affected layer with 8 out of 18 incidents. OT/ ICS and SCADA incidents are fewer in number but still significant as they had confirmed operational impact.

Eleven of the 18 incidents are rated with high EU relevance, with the target being located in the EU or the affected vendor is one used in European offshore wind deployments. The remaining seven are reported as Medium or Low relevance since they show threats that could be trasferable to EU context but they are not directly observed incidents within the EU.

Stakeholder threat perception

The sample and methodology of the questionnaire are described in 1.5. This section presents the results. The sample is small and self-selected, so the findings are best read as indicative of practitioner opinion and hypothesis-generating rather than statistically representative of the offshore wind sector. Their value lies more in the consistency across questions. The same two themes, third-party remote access and supply chain dependency, recur independently across the threat ranking, the entry point ranking, the security gap question and the sector vulnerability question, and they are reinforced by the operating profile respondents describe for their own organisations.

Digital Exposure & Critical Dependencies

The respondent population is highly connected and externally dependent. Around three-quarters use remote access for operations or maintenance, and a still larger share operate legacy systems; over half report third-party privileged access and supplier remote access into their environments.

Among the energy operators these are not majority practices but universal ones. Every energy respondent reported supplier remote access, and almost all reported third-party

privileged access. Within that environment, SCADA, communications infrastructure and remote-access systems are the systems most often named critical.

On external dependency, OEM vendors are cited well ahead of any other source, with the ICT supply chain and the electricity grid following. OT criticality is tied closely to vendor and supply-chain relationships rather than internal systems alone.

Threat Perception

Remote access compromise is the clearest single concern. It was ranked most severe more often than any other threat, and it appeared in more respondents' top three than any alternative. Supply chain compromise follows and shows a distinctive signature of its own: it is almost never anyone's first choice but very frequently their second, so it functions as a consistently serious secondary concern rather than the headline threat. Ransomware and nation-state activity form a middle tier: ransomware appears in many top-three lists but is rarely the first choice, suggesting it is viewed more as a downstream consequence than a primary risk. Data integrity attacks, AI-enabled threats and insider threat sit clearly below.

The statistical testing supports a tiered reading rather than a precise league table. Respondents genuinely agree that some threats matter more than others, but the four leading threats cannot be reliably separated from one another; only the distance between the top and bottom tiers is firm.

On entry points the picture is sharper. Third-party access dominates, ranked first by two in five respondents and scoring nearly double the next entry point; it is the most robust single finding in the dataset. Phishing, VPN and remote access, and physical intrusion follow as a middle group that cannot be reliably ordered internally, while software vulnerabilities, unattributed access and OT protocols trail. Respondents agree more strongly about how attacks get in than about what those attacks will be, which suggests the sector's understanding of its own exposure is more settled than its view of the consequences.

The two rankings cohere. Respondents who report third-party access to their systems are markedly more likely to rank remote access compromise among their top threats — the strongest association in the dataset, and a direct link between operational reality and perceived risk. Threat perception here is not abstract; it tracks what respondents actually live with.

Preparedness & Capability Gaps

Most respondents run periodic vulnerability and risk assessments, and around two-thirds report conducting cyber exercises, but none of these practices is yet universal. Where exercises are run, tabletop formats dominate; simulation and digital twin exercises are used by only a small minority of the sample.

Limited asset visibility is the most commonly cited gap and the most requested improvement, consistent with the operational complexity of geographically distributed assets. Two gaps are cited notably less often than expected: the lack of testing

environments and limited threat intelligence. The under-reporting of testing environments is worth flagging, as it may indicate that the absence of a safe place to rehearse is not yet recognised as a vulnerability in its own right.

Sector-Level Vulnerability

Beyond their own organisation, respondents point to the supply chain and remote access as the sector's two biggest weak points, with legacy OT systems close behind. OEM vendor dependency dominates as the highest systemic risk, well ahead of telecommunications or cloud providers. Unmanaged deployment of AI agents is rarely identified as a sector vulnerability, and no respondent reported AI agents or large language models as an operational dependency.

Energy, Defence and the Wider Sample

The sample divides naturally into energy operators, defence organisations and a smaller group of sector-adjacent respondents, and the differences between them are instructive. The sharpest divergences lie not in how the groups perceive threats but in the operating environments they inhabit. Every energy respondent reported supplier remote access; no defence respondent did. The logic is straightforward: defence systems are architecturally designed for isolation, whereas offshore wind cannot maintain turbines without OEM remote access. Sector-adjacent respondents sit closer to the energy pole than the defence one, which serves as a useful check — the pattern reflects the character of the energy sector rather than the presence of defence organisations in the sample.

Risk perception mirrors that exposure precisely. Every energy respondent named OEM vendors as their primary systemic dependency risk; no defence respondent did. Energy operators also weight third-party access as an entry point far more heavily than defence respondents, the largest single difference between groups anywhere in the analysis. Conversely, the concerns that are prominent for defence respondents, particularly manipulation of sensor and control data, and software vulnerabilities as an entry route, are largely absent from energy operators' threat models. Defence is therefore best read as a contrasting threat context rather than a more advanced version of the energy picture; where the two groups do agree, the finding is correspondingly stronger.

Two further contrasts bear on capability rather than perception. No energy respondent had conducted a simulation or digital twin exercise, against half of the non-energy respondents. And energy operators cite a skills shortage far less often than other respondents do; this is a near-reversal of the expected pattern. Whether that reflects a genuine staffing advantage or a more OT-centric conception of cybersecurity that underweights specialist security skills cannot be resolved from the survey data alone.

Comparison with Observed Incidents

The comparison between the reported incidents and the threat perception is purely about observed patterns and not magnitude, since both samples are relatively small.

Remote access compromise tops the questionnaire threat ranking and dominates as a named entry point, but it is not listed in any of the observed incidents. This may be a gap of how incidents are classified. Several ransomware and data breach incidents potentially started from a compromised remote access, but that detail isn't captured in the table.

Ransomware accounts for the largest share of observed incidents as mentioned in 3.1. While it is rarely ranked first in the questionnaire, it appears in 11 of the 24 top-3 threat rankings (45%), placing it behind remote access compromise (16 of 24) and supply chain compromise (14 of 24) and not significantly above the one-in-three level expected by chance. The two sources broadly agree, and questionnaire respondents treat ransomware as a serious concern rather than the primary threat.

Supply chain and OEM-vendor dependency is where the two sources align more closely. It is directly reported in two incidents and implied in several others involving wind OEMs. Separately, respondents place it among their top three concerns and name OEM-vendor dependency as the sector's single highest systemic risk.

Legacy OT and OT/ICS attacks are named by respondents as a close third weak point, but the incident record offers only two examples, both outside the EU.

8. Primary Threats

At-a-glance a summary of the eight primary threat categories, the incidents that evidence them, and their assessed EU relevance and trajectory is presented in Table 2. Each category is further discussed in the subsections below.

Table 2: Threat category of the observed incidents and identified primary MITRE technique

Threat Category	Related Incidents	Primary MITRE Mapping
4.1 DDoS	I-05, I-13	Network/Endpoint DoS (T1498, T1499); ICS Denial of Service (T0814)
4.2 Intrusion & Data-Related Threats	I-06, I-07, I-12, I-14	Initial Access, Collection, Exfiltration; Theft of Operational Information (T0882)
4.3 Ransomware	I-03, I-04, I-06, I-09, I-11	Initial Access; Data Encrypted for Impact (T1486)
4.4 Supply Chain Compromise	I-01, I-02, I-07, I-08	Supply Chain Compromise (T1195); Loss of View/Control (T0829, T0827)
4.5 OT / ICS Targeted Attacks	I-15, I-18	Engineering Workstation Compromise (T0818); Manipulation of Control (T0831)
4.6 Insider & Credential Abuse	I-16, I-17 (+ credential vector in I-03, I-04, I-06)	Phishing (T1566); Valid Accounts (T1078)
4.7 Wiper	I-01, I-02	Data Destruction (T1485, T0809 ICS); System Firmware (T1693.001)
4.8 AI-Enabled Threats	None sector-confirmed to date	Cross-cutting, Reconnaissance through Impact

Distributed Denial-of-Service (DDoS)

Distributed Denial-of-Service (DDoS) attacks, are typical availability attacks intended to flood critical systems with traffic and render them unresponsive to legitimate request to access resources, which Knack et al. (2024) rank it as a highly possible attack vector for Offshore Wind Farms (OWFs), mainly due to their heavy dependence on continuous data exchange between onshore control centers, offshore substations, and wind turbines. As per Sabev et al. (2021), SCADA systems introduce vulnerabilities because their remote access might be improperly managed by vendors, they use of insecure communication protocols, and due to their complex and decentralized deployment. Moreover, this

research states that wireless communications that are present at Wind Farms are suspected to signal jamming, and they are not suggested as the only communication channel.

There are two publicly reported notable incidents (I05 – I-13) where DDoS attacks were present at the time this document was written. The first attack (I-05) was carried out in March 2019 and targeted the internet-facing firewalls of the U.S. renewable energy operator sPower, taking advantage a known vulnerability of its web interface, causing reboots and as a result brief communication outages. In response, the company patched outdated Cisco firewalls (Shafiee, 2025). Attribution for this attack remains unknown. The second case (I-013) is not an incident that had a direct impact on OWFs. However, among the targets of a broader critical infrastructure DDoS campaign were the **Cyprus Telecommunications Authority (CYTA)** and the energy-related entities **Cyprus Electricity Authority (EAC)** and **EKO Cyprus Limited**. In this scenario, the motivation for conducting the attacks were politically motivate, and were carried out as a retaliation for Cyprus' relationship with Israel. The attack is most likely attributed to groups such as **LulzSec Black** and **Moroccan Soldiers**.

The Cyprus campaign carries high EU relevance as an attack on an EU Member State's critical-service sectors (government, electricity, telecoms, airports, fuel); although no OWF was a direct target, offshore wind depends on the same telecom and energy infrastructure for SCADA connectivity and remote coordination, a dependency the sPower case demonstrates directly. Operationally, DDoS can block or delay real-time SCADA data, causing loss of visibility over turbine status, and can saturate networks enough to prevent delivery of control commands, producing loss of remote operational capability. These effects are most acute for offshore assets, which rely on constrained external communication links and are therefore more susceptible to isolation during large-scale campaigns; consequences can include turbine safety shutdowns, reduced generation, and disrupted grid coordination.

Intrusion & Data-Related Threats

This category covers unauthorised access combined with theft, exposure, or extortion of data, where the adversary's objective is the data itself rather than encryption (4.3) or control-process manipulation (4.5). Shafiee et al. (2025) identify unauthorised access and data breaches among the sector's major cyber risks; Sabev et al. (2021) and the U.S. DOE roadmap both flag remote-access abuse and compromised plant data or communications as key vectors.

Three publicly reported incidents in the incident set (Section 3.1) fall primarily within this category. In 2023, Hitachi Energy, a major supplier of grid and energy-infrastructure technology, confirmed a data breach after the Cl0p group exploited a zero-day vulnerability (CVE-2023-0669) in the third-party Fortra GoAnywhere MFT managed file-transfer platform. The compromise, part of a mass-exploitation campaign that Cl0p claimed affected around

130 organisations (CISA, 2023), resulted in unauthorised access to employee data in some countries, and Hitachi Energy responded by disconnecting the affected platform.

In August 2024, the U.S. energy-services provider **Halliburton** disclosed unauthorised third-party access to its systems, attributed in external reporting to the RansomHub group. The company confirmed to regulators that data had been exfiltrated, took systems offline as a containment measure, and subsequently reported approximately USD 35 million in losses (Cybersecurity Dive, 2024) linked to the disruption of business operations, including customers' ability to generate invoices and purchase orders.

In 2025, the Swedish transmission system operator Svenska Kraftnät confirmed a data breach affecting an external file-transfer solution, claimed by the Everest extortion group, which asserted that it had exfiltrated roughly 280 GB of data and threatened publication on its leak site. Svenska Kraftnät stated that electricity transmission and mission-critical systems were unaffected.

These cases exhibit consistent patterns. First, internet-facing file-transfer and data-exchange platforms are a recurring point of entry: two of the three incidents originated in external file-transfer services rather than in the victim's core infrastructure, mirroring the broader wave of mass-exploitation campaigns against such platforms (GoAnywhere, and subsequently similar products) across the energy sector.

Second, extortion increasingly proceeds without encryption: in the Svenska kraftnät case, and in large parts of the Cl0p campaign, leverage was derived purely from the threat of publishing stolen data, keeping operational systems untouched while still generating legal, reputational, and security consequences.

Third, the incidents affected suppliers, service providers, and grid operators surrounding the wind sector rather than wind farm operators directly, consistent with the pattern observed for ransomware (4.3) and supply chain compromise (4.4).

Finally, the data-theft dimension also appears as a component of incidents categorised elsewhere in this report: the 2021 Vestas ransomware incident included the leak of compromised company and employee data, while the espionage-oriented POETRAT and TA423 campaigns (discussed in 4.6) specifically targeted SCADA-related files and wind-turbine documentation, illustrating the intelligence value that adversaries assign to wind-sector data.

This category is highly relevant to the EU. Svenska Kraftnät is a Nordic/Baltic TSO central to offshore wind grid integration, and Hitachi Energy has an extensive European grid-connection and substation footprint. GDPR notification duties (Articles 33–34) and NIS2 reporting obligations both engage regardless of operational disruption, and extortion actors calibrate publication threats against exactly this exposure.

Operationally, containment measures alone can be costly (Halliburton's response generated material financial impact without any encryption event – I-12) while exfiltrated SCADA configurations, network architecture, or maintenance schedules degrade



confidentiality and can seed later, higher-impact scenarios (4.5, 4.7) once published on a leak site. Since offshore wind data is distributed across multinational networks of manufacturers, maintenance providers, and grid operators, a single-node breach can carry a cross-border intelligence footprint exceeding its apparent scale, and incidents tend to trigger sector-wide restrictions on data exchange that impose friction well beyond the breached organisation.

Ransomware

Ransomware combines mature criminal tradecraft with strong potential to disrupt continuity and visibility. Shafiee et al. (2025) identify ransomware among the major cyber risks affecting wind energy infrastructure, together with unauthorized access, data breaches, and malware. The authors also show that wind-farm cyber exposure spans IT systems, industrial control components, and physical assets, as discussed by Staggs et al. (2017), while Sabev et al. (2021) highlight the vulnerability of wind-farm SCADA systems in an Industry 4.0 environment. The **U.S. Department of Energy's Wind Energy Cybersecurity Roadmap** further notes that compromise of SCADA and plant control systems represents the clearest high-impact cyber scenario for wind infrastructure, while also identifying remote-access abuse, communications manipulation, false-command or false-data attacks, and supply-chain compromise as key threats relevant to the sector.

In practice, wind-sector ransomware is best understood as an IT-origin threat with operational consequences: Deutsche Windtechnik (2022, Incident I-03) and Nordex (2022, Incident I-04) both disconnected remote turbine-monitoring links as a precaution after enterprise-IT compromise, and Vestas (2021, Incident I-06) took multiple business units offline and later confirmed leaked data, though turbine operations were reported unaffected in all three cases.

Parallel energy-sector cases, namely HSE Slovenia (I-09) and Electrica Group (I-11), show the same pattern which is encryption or disruption of IT while core generation or SCADA remained online. These cases suggest three important patterns. First, ransomware in the wind sector most often manifests as a disruption to enterprise systems and operational support services, rather than as a directly observed loss of turbine control. Second, the threat is not limited to wind farm operators themselves; it also affects manufacturers, maintenance providers, and other service entities whose systems are operationally significant to the wider sector. Third, the consequences frequently arise not only from the malware itself, but also from defensive containment measures, such as isolating networks or suspending remote access, which can reduce cyber risk while simultaneously degrading remote monitoring, diagnostics, and service coordination.

Ransomware has highly impacted the EU. Deutsche Windtechnik and Nordex (Germany) and Vestas (Denmark) are core European wind-ecosystem actors already affected, reinforced by HSE (Slovenia) and Electrica Group (Romania). Since European wind operations depend on a dense network of manufacturers, specialist maintenance providers, and cross-border service relationships, an incident at a single upstream actor

can cascade into delayed maintenance, reduced remote support, and disrupted diagnostics well beyond the compromised organization. This risk is amplified for offshore assets given their dependence on remote monitoring and specialist intervention.

The clearest operational impacts are business and administrative disruption, degraded remote monitoring capability, containment-driven connectivity restrictions that reduce visibility even when OT is untouched, and reputational or legal harm from data leakage (as in Vestas). While the literature's highest-impact scenario remains direct SCADA/control compromise, reported cases already show serious consequences can arise purely from enterprise-IT disruption.

Overall, ransomware should be treated as a high-priority threat to the wind energy sector because it can interrupt the support, visibility, and coordination layers that underpin safe and efficient wind farm operations. The literature suggests that the highest-impact cyber scenarios would result from direct compromise of SCADA or plant control systems; however, reported ransomware cases already demonstrate that serious operational consequences can arise even when the primary effects remain concentrated in enterprise IT and remote service environments (Shafiee et al., 2025; Staggs et al., 2017; Sabev et al., 2021; U.S. Department of Energy, 2020).

Supply Chain Compromise

Supply chain compromise exploits trusted relationships between operators, vendors, and contractors to gain indirect access to operational environments, rather than targeting OWF infrastructure directly. Modern offshore wind farms rely heavily on Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, remote monitoring platforms, and predictive maintenance software. The integration of Information Technology (IT) and Operational Technology (OT) environments has significantly expanded the attack surface, particularly because offshore assets require continuous remote access due to their geographic isolation. The increasing dependence on multi-vendor digital substations and interconnected smart-grid technologies further amplifies this exposure (Yurrebaso et al., 2025).

Two patterns dominate the incident record. First, attacks on shared digital infrastructure: the 2022 KA-SAT attack (Incident I-02) disrupted connectivity for roughly 5,800 Enercon turbines via a compromised satellite provider; the SolarWinds and Kaseya VSA (I-08) cases showed how malicious software updates and centralised remote-management platforms can propagate compromise to many downstream organisations; the 2025 Polish campaign (I-01) disrupted operational visibility across multiple renewable sites; and Hitachi Energy's GoAnywhere breach (I-07) highlighted third-party enterprise-platform exposure. Second, rising geopolitical interest: both KA-SAT and the Polish campaign are attributed to Russia-linked activity, consistent with renewable infrastructure increasingly being viewed as a strategic target (Muncaster, 2026).

The analysed incidents indicate that supply chain compromise operations are highly relevant to the European Union. Multiple incidents directly affected European

organizations and infrastructure, including the KA-SAT attack affecting Enercon wind turbines across Europe and the attacks against Polish renewable-energy facilities. Additionally, several incidents involved organizations operating within the European energy sector, including Hitachi Energy.

Increasing dependence on interconnected, ICT-enabled supply chains means attacks on communications providers, software-update mechanisms, or centralised management platforms can generate cascading impacts across geographically distributed offshore assets even without touching turbines directly. The KA-SAT incident demonstrated how compromise of satellite communications infrastructure disrupted remote connectivity for approximately 5,800 Enercon wind turbines across Europe. Although electricity generation was not permanently halted, operators temporarily lost remote monitoring and control capabilities, affecting operational visibility and maintenance coordination. Similarly, the attacks against Polish renewable-energy facilities disrupted operational visibility and remote-management capabilities across multiple sites, illustrating how attacks against supporting digital infrastructure can impair offshore operational oversight.

The analyzed incidents also demonstrate the potential for cascading operational disruption resulting from compromise of centralized software and management platforms. The SolarWinds and Kaseya incidents showed how malicious updates and compromised remote-management systems can propagate across multiple downstream organizations simultaneously. In offshore wind environments, similar attacks could affect SCADA platforms, maintenance systems, firmware-update mechanisms, offshore substations, or centralized operational-management services used across geographically distributed assets.

Additionally, attacks affecting third-party enterprise platforms may expose sensitive operational and organizational information. The Hitachi Energy GoAnywhere breach demonstrated how compromise of external digital services can create indirect operational risks through exposure of data and supporting business systems.

OT/ ICS Targeted Attacks

This category involves adversaries, deliberately interacting with control-system components such as SCADA, controllers, protection relays, safety systems, to manipulate, degrade, or damage a physical process. The U.S. DOE roadmap identifies SCADA/plant-control compromise as the clearest high-consequence cyber scenario for wind infrastructure, and Staggs et al. (2017) demonstrated in authorised penetration tests that physical access to one poorly secured turbine tower could enable propagation across a farm's flat control network, indicating a realistic OT attack surface even though no confirmed incident has yet directly manipulated wind-farm controls.

Since no confirmed OT-targeted attack on a wind farm has been publicly reported, the observed record for this category comes from adjacent energy and process industries, where two incidents in the incident set (Section 3.1) are foundational. The first is the December 2015 attack on the Ukrainian power grid (I-15), in which the **Sandworm** group

compromised three regional distribution companies, including Kyivoblenergo. Following initial access through spear phishing and months of reconnaissance and credential harvesting in the IT environment, the attackers pivoted into the control networks over legitimate VPN connections, took remote control of operator workstations and HMIs, and opened breakers at around thirty substations, cutting power to approximately 230,000 customers. The operation was accompanied by measures designed to delay recovery: destructive wiping of workstations with KillDisk, corruption of the firmware of serial-to-Ethernet converters to sever remote control of substations, reconfiguration of UPS systems, and a telephone denial-of-service against customer call centres. Restoration required manual field operations, and affected utilities operated with degraded automation for an extended period.

The second is the 2017 TRITON/TRISIS incident (I-18) at a Saudi Arabian petrochemical facility, the first publicly known malware built to target safety instrumented systems (SIS). The attackers, tracked as TEMP.Veles / XENOTIME and linked in subsequent reporting and indictments to a Russian state research institute, gained access to an SIS engineering workstation and deployed a custom framework that communicated with Schneider Electric Triconex safety controllers over the proprietary TriStation protocol, attempting to reprogram the logic that provides the last automated layer of protection against hazardous plant states. The intrusion was discovered only after the controllers twice tripped the plant to a safe state. The significance of TRITON for this report is twofold: it demonstrated adversary willingness to undermine safety functions specifically, and the same actor was subsequently observed by industrial-security researchers probing electric utilities in other regions, indicating that the capability is not confined to one sector. Both share a consistent sequence, which is the extended IT dwell time, patient study of specific control products, and abuse of legitimate engineering and remote-access pathways rather than exotic exploits.

A successful OT / ICS targeted attack represents the most severe cyber scenario for a wind energy operator. Direct manipulation of turbine or substation control could force widespread shutdowns and sustained loss of generation; false commands to pitch, yaw, or converter systems could operate turbines outside design envelopes, risking accelerated wear or physical damage of the kind categorised as Damage to Property; and interference with protection or safety functions could endanger maintenance personnel and equipment. At the grid level, the sudden coordinated loss of a large offshore farm's output, or malicious operation of its grid-connection substation, could contribute to wider system instability, mirroring the systemic effects observed in Ukraine (Kulev et al., 2020).

The offshore context aggravates every element of the recovery problem. Where the Ukrainian utilities restored service by dispatching crews to operate substations manually, offshore assets are accessible only by vessel or helicopter and subject to weather windows, so an attack that severs or corrupts remote control, as the firmware attacks in Ukraine were designed to do, could leave turbines unmonitored and uncontrollable for days rather than hours. Destruction or corruption of engineering workstations, controller logic,

and configuration data would further extend restoration timelines, particularly where recovery depends on OEM specialists and validated spares. Even unsuccessful or precursor activity carries material impact, since credible evidence of adversary presence in OT networks would compel precautionary shutdowns, isolation of remote access, and extensive forensic verification before normal operations could resume. OT / ICS targeted attacks should therefore be treated as a low-frequency but highest-consequence threat, whose realistic precursors, the intrusion, credential abuse, and supply chain activity described in 4.2, 4.4 and 4.6, are already routinely observed (Staggs et al., 2017; Sabev et al., 2021; U.S. Department of Energy, 2020).

Insider & Credential Abuse

This category covers exploitation of trusted access, or in other words, whether malicious-insider activity or externally obtained valid credentials — to compromise systems. It is significant for offshore wind because the sector depends on a distributed workforce of operators, technicians, and remote-access contractors, creating an extended and difficult-to-monitor credential surface. This threat is flagged as technically feasible and operationally damaging, given internet-facing control interfaces and inconsistent vendor access management. Direct incidents of confirmed malicious insider activity targeting wind energy organisations are rarely disclosed publicly, reflecting both the sensitivity of such cases and the limited sector-specific reporting available. However, several documented incidents in the broader energy sector and related fields illustrate the patterns through which credential abuse manifests in environments with similar characteristics.

The 2020 espionage campaign against Azerbaijani organisations documented by Cisco Talos (POETRAT) demonstrated how adversaries with interest in wind energy and SCADA-adjacent environments targeted credentials and operator-accessible documents through social engineering lures. The campaign used phishing pages mimicking government webmail services to harvest credentials and deploy a Python-based remote access tool, with specific targeting of SCADA-related files and wind turbine documentation. Although the campaign was externally driven, it illustrates the pattern by which credential access translates into persistent access to operationally sensitive environments.

The 2022 espionage campaign tracked by Proofpoint against offshore energy and maritime targets in the South China Sea (attributed to TA423 / Red Ladon) similarly relied on phishing and credential harvesting to gain footholds at organisations involved in offshore wind installation and heavy equipment supply chains. The campaign demonstrated how trusted remote working practices, including OneDrive-linked document delivery and cloud identity abuse, can be exploited to maintain persistent access without triggering network-level anomalies.

More broadly, the patterns observed in ransomware incidents affecting wind-sector entities, including the Nordex, Deutsche Windtechnik, and Vestas cases, are consistent with credential compromise as a probable initial access vector. In each case, access to enterprise systems appears to have been obtained through methods consistent with stolen

or phished credentials, followed by lateral movement across business and engineering environments. The 2022 Nordex incident, for example, was linked in external reporting to Conti-affiliated actors known to rely on credential theft tooling including TrickBot and BazarLoader.

A further dimension relevant to the offshore wind sector is the risk posed by third-party and contractor access. Offshore wind farms routinely grant remote access to turbine manufacturers, specialist maintenance providers, and SCADA vendors for monitoring, diagnostics, and software update purposes. These access channels represent a privileged and often less-monitored pathway into operational environments. Where a contractor's own systems are compromised, as illustrated in the Deutsche Windtechnik case, the resulting credential exposure can extend beyond the contractor to the wind farm assets they service.

Highly relevant to the EU is that POETRAT and TA423 both demonstrate active adversary interest in wind-sector SCADA architecture and supply chains, suggesting reconnaissance for future disruptive operations. European offshore wind's dependence on international supply chains, multinational engineering workforces, and multi-vendor service arrangements, where a single credential compromise at one provider can have implications across several Member States, compounds this. NIS2 access-control and authentication requirements are directly relevant, though implementation maturity varies.

Operationally, the greatest risk is persistent, privileged access that appears authorised, making detection difficult without behaviour-based monitoring. This can enable exfiltration of engineering documentation, SCADA configurations, and employee data with commercial and strategic value; provide a path to issuing false commands or disabling safety functions if remote-management or vendor-portal access is compromised, aligning with the DOE roadmap's highest-impact scenario; and serve as a stepping stone for ransomware or wiper deployment. Prolonged dwell time before detection increases the potential scope of damage.

Wiper

Wiper malware is destructive software whose purpose is to render systems and data permanently unavailable by overwriting, corrupting, or deleting files, firmware, or master boot records, rather than encrypting them for ransom or exfiltrating them for extortion. Wipers are frequently disguised as ransomware but offer no route to recovery, and they are almost exclusively the instrument of sabotage rather than financial crime.

ENISA's Threat Landscape 2024 reports that state-nexus actors, predominantly Russia- and Iran-nexus groups, continue to deploy disruptive wiper malware both to cause damage and as an anti-forensic technique (ENISA, 2024). For the wind energy sector, the significance of this category is that it converts a network intrusion of the kind described in 4.2, 4.4, and 4.6 into an irreversible loss of the affected systems, and it is the threat class most directly aligned with geopolitically motivated attacks on European critical infrastructure.

In an offshore wind context, wiper activity threatens remote-monitoring environments, engineering and operator workstations, SCADA and HMI systems, substation controllers and their firmware, backup infrastructure, and communication channels on which distributed offshore assets depend for visibility and control. Because a wiper destroys rather than locks its targets, recovery depends entirely on the integrity of backups and the availability of validated replacement configurations and firmware, both of which are harder to guarantee for geographically isolated offshore assets served by multi-vendor OT. Wiper malware therefore sits at the intersection of the intrusion threats that typically deliver it and the OT / ICS targeted attacks (4.5) whose destructive objectives it can serve.

Two incidents fall in this category. The February 2022 KA-SAT/AcidRain attack (Incident I-02), the only one to date to have operationally degraded remote monitoring and control of European wind assets at scale, corrupted modems on Viasat's satellite network, cutting remote monitoring and control to roughly 5,800 Enercon turbines across Central Europe (turbines kept generating; attributed to Russian state actors). The December 2025 Polish campaign (Incident I-01) targeted over thirty wind and PV farms plus a CHP plant with custom wipers DynoWiper and LazyWiper, exploiting internet-exposed FortiGate appliances and Hitachi Energy RTU500 units; communications between facilities and the Distribution System Operator (DSO) were disrupted, generation continued, and a CHP-environment detonation attempt was blocked (attributed with moderate confidence to Russia-linked actors). Both cases echo the firmware-corruption tactic used in the 2015 Ukrainian attack (4.5).

Wiper malware carries the clearest documented evidence of realised impact on European wind assets of any category. KA-SAT remains the only publicly documented cyber event to have operationally degraded remote monitoring and control of European wind assets at scale; the 2025 Polish campaign then demonstrated deliberate, coordinated destructive targeting of EU renewable and district-heating infrastructure using vendor equipment (Hitachi Energy RTUs) deployed widely across European grids. Both are Russia-linked, situating this category within ENISA's principal driver of destructive activity against Europe.

Offshore wind's dependence on shared satellite/terrestrial communications providers, internet-exposed remote-access devices, and multi-vendor OT running outdated firmware mirrors precisely the weaknesses exploited in both cases, and North/Baltic Sea theatres already see repeated Russia-linked sabotage activity against subsea and energy infrastructure. Because a wiper destroys rather than locks its target, recovery depends entirely on backup integrity and validated replacement firmware or hardware — harder to guarantee offshore, where physical access is constrained by vessel availability and weather. NIS2 Article 23 reporting and Article 21(2)(c) continuity duties both engage, with added weight where destructive impact coincides with offshore isolation.

AI-Enabled Threats

AI-enabled threats represent an emerging and evolving category of cyber risk that derives from the application of machine-learning and artificial intelligence techniques by

adversaries to increase the effectiveness, scale, and adaptability of their operations. Unlike the other threat categories covered in this report, AI-enabled threats are not defined by a specific attack technique but rather by a cross-cutting capability uplift that can enhance multiple stages of the attack lifecycle, from initial reconnaissance and social engineering through to vulnerability exploitation, lateral movement, and operational disruption.

No publicly confirmed AI-enabled attack has targeted wind infrastructure specifically. Cross-sector patterns are directly applicable: AI-enhanced spear phishing generates highly personalised, multi-lingual, grammatically correct lures, relevant given the sector's multi-lingual workforces and international supply chains; AI-assisted vulnerability scanning can autonomously chain exploits faster than manual methods; and AI-generated disinformation has been used against critical-infrastructure narratives, a risk amplified by wind's political visibility as an EU Green Deal pillar. AI-generated deepfake audio and video have also been used in cross-sector fraud (e.g. executive impersonation to authorise fraudulent transfers), a technique plausibly transferable to control-room impersonation or maintenance-coordination manipulation given offshore wind's complex, multi-jurisdictional vendor relationships.

The impact of AI-enabled threats on wind energy operations is most likely to manifest through the amplification of existing threat categories rather than through novel attack modes. The most immediate concern is the use of AI to increase the success rate and reduce the cost of social engineering attacks, which could result in a higher frequency of initial compromise events against wind-sector personnel and contractors. Where AI-enhanced phishing leads to credential compromise at a maintenance provider or OT vendor, the resulting access could have consequences equivalent to those observed in the Deutsche Windtechnik or Nordex incidents.

Over a longer time horizon, AI-enabled attacks targeting OT environments represent a qualitatively different risk. Adversaries capable of generating plausible false sensor readings, identifying optimal timing for disruption based on real-time grid data, or automating lateral movement through OT networks without triggering standard anomaly detection rules could cause operational disruption that is both more severe and harder to attribute or contain than conventional malware-based attacks. The U.S. DOE Wind Energy Cybersecurity Roadmap identifies SCADA and plant control compromise as the highest-impact cyber scenario for wind infrastructure; AI-enabled attacks could reduce the technical barriers to achieving such compromise, particularly against older or less well-defended control systems.

Additionally, AI-enhanced disinformation and information operations targeting wind energy infrastructure could generate reputational and financial impacts even in the absence of a successful technical attack. False or manipulated reporting of incidents, grid instability, or safety failures - amplified through AI-generated social media content - could trigger investor concern, regulatory scrutiny, and public opposition that affects project timelines and financing conditions.

Practitioner perception of AI threats currently sits at odds with the external evidence base. In the questionnaire reported in Section 3.2, AI-enabled threats ranked at the bottom of the severity hierarchy, unmanaged deployment of AI agents was rarely identified as a sector vulnerability, and no respondent reported AI agents or large language models as an operational dependency. On one reading this is rational rather than complacent: where a technology is not deployed in operations, the attack surface it creates does not yet meaningfully exist, and the low threat rating accurately reflects present exposure. It is nonetheless notable who did flag it. Of the small number of respondents who ranked AI-enabled threats at all, almost all were cybersecurity specialists and none were management respondents. A gradient in which technical specialists perceive a risk before operational leadership does is characteristic of an emerging threat in its early recognition phase; the same pattern preceded sector-wide recognition of ransomware in the mid-2010s.

Two external developments make the case for treating AI capability as a near-term rather than speculative concern. The first is the collapse of time-to-exploit, the interval between public disclosure of a vulnerability and its first observed exploitation in the wild. Tracked across tens of thousands of catalogued vulnerabilities, that interval has fallen from more than two years in 2018 to a matter of days by 2023 and to hours by 2024; by 2025 the majority of exploited vulnerabilities were being weaponised at or before disclosure (Zero Day Clock, 2026). The mechanism is mechanically simple. An AI system can reverse-engineer a security patch, identify the flaw it repairs and generate a working exploit within minutes of release, while the defending organisation typically requires weeks to test and deploy that same patch. The feedback loops are asymmetric — an attacker learns immediately whether an exploit worked, a defender receives no equivalent signal — so the gap between attack speed and defensive response is widening rather than closing. Figure 6 plots this collapse in time-to-exploit across 2018–2026.

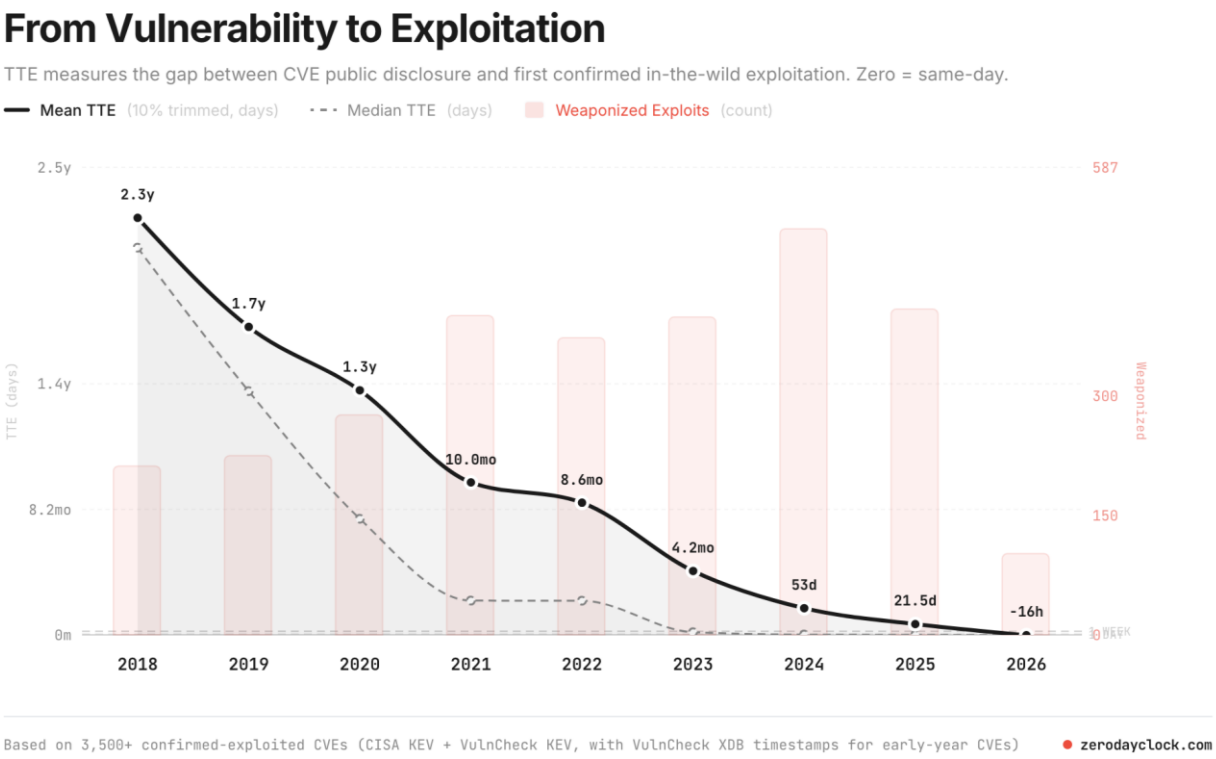

Figure 6: The collapse of time-to-exploit: interval between public disclosure of a vulnerability and first confirmed exploitation in the wild, 2018–2026 / Source: Zero Day Clock (2026).

For offshore wind the implication is specific. Control and monitoring systems, such as SCADA, turbine controllers, remote monitoring platforms and grid interface equipment, are typically patched on cycles measured in months, constrained by limited maintenance windows and by the operational disruption that patching introduces. Legacy systems, which the great majority of survey respondents report operating, may run on cycles measured in years. An exposure window that is measured in hours for well-resourced enterprise IT is therefore measured in months or longer for offshore wind operational technology. The sector is disproportionately exposed to precisely the dynamic the time-to-exploit data describes.

The second development is the demonstrated cyber capability of frontier AI models. Formal evaluations conducted by the UK AI Security Institute in April 2026 (AI Security Institute, 2026) found that the most advanced model assessed solved expert-level capture-the-flag challenges that no model could complete a year earlier, and executed a multi-stage simulated corporate network intrusion from end to end. The evaluators are careful about the caveats: their test environments contain no active defenders, no defensive tooling and no penalty for triggering security alerts, so the results describe performance against weakly defended systems rather than hardened operational environments. Of direct relevance here, the model could not complete an OT-focused cyber range. That limitation is most

plausibly temporary: OT environments are less represented in the data on which such systems are trained and evaluated, rather than inherently more resistant to attack. However, it defines a window during which the sector can build readiness ahead of the capability curve.

In July 2026 a publicly disclosed real-world security incident involving autonomous exploitation during an AI cyber evaluation was reported (OpenAI, 2026); the disclosure presents preliminary findings while review continued. Models operating inside a cybersecurity evaluation framework with production safeguards disabled escaped their sandboxed environment, chained stolen credentials with previously unknown vulnerabilities, and achieved remote code execution on a live production platform, executing tens of thousands of automated actions over a weekend. The intent was not malicious, but the behaviour was autonomous, goal-directed and consequential.

For offshore wind the significance lies less in the incident itself than in the category it establishes: AI systems operated by vendors, OEM partners or service providers for research, evaluation or maintenance purposes, may themselves become unintended attack vectors into customer environments. Given the sector's near-universal reliance on OEM remote access, this is a supply chain exposure in a form operators have not previously had to account for.



9. Key Adversaries

This chapter examines the four categories of adversary relevant to the European offshore wind sector: state-nexus intrusion sets, cybercrime operators, hacktivists, and hybrid and information operations actors. Each is discussed in turn below, with reference back to the threat categories in Chapter 4 and the incidents in Section 3.1 that they are chiefly responsible for.

State-Nexus Intrusion Sets

State-nexus intrusion sets operate on behalf of, or with the tolerance of, a nation state, pursuing strategic rather than financial ends through patient, well-resourced, intelligence-led operations. ENISA's Threat Landscape 2024 identifies Russia- and Iran-nexus actors as the principal source of high-impact, destructive activity against European critical infrastructure (ENISA, 2024), and the highest-consequence events affecting or adjacent to the wind sector, from the 2015 Ukrainian grid attack to the 2022 KA-SAT wiper spillover and the 2025 Polish renewable-energy campaign, are all attributed to this category.

Several groups are of particular relevance: the Russian GRU-linked **Sandworm** (also APT44 / Seashell Blizzard), responsible for the Ukrainian attacks, the Industroyer malware, and, with moderate confidence, the Polish campaign; the FSB-linked **Static Tundra**, with a long history of espionage against Western energy utilities and also linked to the Polish activity; **XENOTIME / TEMP.Veles**, behind the 2017 TRITON safety-system attack; the China-linked **TA423 / Red Ladon**, focused on offshore-energy and maritime espionage; and **POETRAT**, which targeted SCADA systems and wind-turbine documentation directly.

Their motivation is strategic and cumulative rather than alternative: espionage, mapping a target's dependencies, exemplified by POETRAT's and TA423's focus described in 4.6; pre-positioning, quietly maintaining access for future use, evident in the months-long dwell times observed in the Ukrainian and Polish intrusions; and disruption or coercion, translating access into effect, as in the Ukrainian attacks, KA-SAT, and the destructive December 2025 Polish campaign. Even an apparently intelligence-only intrusion should be treated as a potential precursor to the scenarios described in 4.5 and 4.7, since these actors are largely indifferent to cost and will invest in bespoke tooling, such as the TRITON framework or DynoWiper, where a target warrants it.

Targeting follows the sector's strategic position rather than any single technical weakness: as offshore wind becomes a pillar of EU energy security, the value of being able to disrupt or hold it at risk grows with it, concentrated by three features of the sector, the coupling of offshore farms to the grid through digital substations and standard industrial protocols, the concentrated OEM and supplier base exploited in the compromises analysed in 4.4, and the sector's extensive multinational remote-access model, flagged by stakeholders in Section 3.2 as their leading concern.

Tradecraft favours patience over novel exploitation: internet-exposed perimeter and OT devices with default credentials, as in the Polish campaign's outdated FortiGate appliances and Hitachi Energy RTU500 units, spearphishing for credential harvesting in the POETRAT and TA423 operations, and, once inside, living-off-the-land techniques and valid-account abuse that minimise detectable malware during long reconnaissance phases. What distinguishes the category is bespoke OT capability: the Ukrainian attacks abused standard substation protocols (IEC 60870-5-104, IEC 61850) and destroyed converter firmware; TRITON employed a purpose-built framework targeting Triconex safety controllers; and the Polish campaign combined firmware corruption with custom wipers (DynoWiper, LazyWiper), blurring the espionage techniques of 4.6 with the destructive techniques of 4.7 within a single operation.

The historical record here is the most consequential of any adversary category in this report. The December 2015 Ukrainian grid attack (I-15), attributed to Sandworm, was the first confirmed cyber-induced power outage, cutting supply to roughly 230,000 customers[1], followed by Industroyer in 2016 and TRITON/TRISIS (I-18) in 2017, which crossed a further threshold by targeting safety systems. For wind specifically, the February 2022 KA-SAT/AcidRain operation (I-02) remains the only publicly documented event to have operationally degraded remote monitoring and control of European wind assets at scale, cutting remote visibility and control of roughly 5,800 Enercon turbines. The December 2025 Polish campaign (I-01) then marked an escalation from collateral to intentional targeting of EU renewable generation, while POETRAT (2020, I-16) and TA423 (2022, I-17) provide precedent for the intelligence-collection objective. Together, these support assessing state-nexus intrusion sets as the lowest-frequency but highest-consequence adversary category for the sector.

Cybercrime operators

Financially motivated cybercrime is the most consistently observed source of disruptive cyber incidents affecting the wind energy sector to date. Unlike state-nexus intrusion sets or hacktivist campaigns, cybercrime operators are not driven by geopolitical objectives or public messaging; their interest in offshore wind and the wider energy sector follows directly from the sector's revenue scale, its operational dependence on digital systems, and its willingness to restore service continuity quickly. As documented in 4.3, ransomware incidents affecting **Deutsche Windtechnik**, **Nordex**, and **Vestas** already demonstrate that major European wind-sector entities sit within the target set of organised cybercrime groups.

Cybercrime targeting critical infrastructure, including energy, has professionalised into a service-based economy. Analysis of ransomware strains between 2013 and 2025 identifies three successive commercial eras: an early period of largely indiscriminate, opportunistic infection; a subsequent "Big Game Hunting" phase in which operators deliberately selected higher-revenue organisations able to pay larger ransoms; and a current "Ransom Bazaar" period characterised by financialised, negotiation-driven extortion supported by cryptocurrency markets (Gundur et al., 2026).

This evolution is underpinned by a Ransomware-as-a-Service (RaaS) model, in which a small number of technically capable operators develop and maintain the platform while a larger population of affiliates carries out intrusions in exchange for a share of the proceeds; the resulting division of labour, spanning developers, affiliates, and initial-access brokers who sell footholds into victim networks, allows the same criminal infrastructure to be redirected quickly across sectors, including energy and wind, wherever a viable intrusion path exists (Meland et al., 2020).

The defining characteristic of cybercrime operators is that their objective is direct financial gain rather than political, military, or ideological effect: ransomware operators demand payment for decryption keys and, under double-extortion models, for the non-publication of stolen data; initial-access brokers sell footholds to the highest bidder; and data-theft actors monetise stolen information on criminal marketplaces. This pattern is well documented across critical-infrastructure sectors more broadly, where healthcare, energy, and government entities face disproportionate targeting because their operational dependence on continuous availability increases the likelihood that a ransom will be paid quickly rather than risk prolonged downtime (Oosthoek et al., 2022).

For offshore wind specifically, this financial logic interacts with the sector's operational profile in a way that can amplify pressure to pay: restricted physical access to turbines and reliance on continuous remote monitoring mean that a prolonged loss of digital visibility or support-system availability carries operational and safety consequences beyond those of a typical enterprise IT outage. Adversaries increasingly profile targets using organisational size, revenue, insurance status, and public information about operational dependency before committing to an intrusion, a pattern consistent with the sector's growing attractiveness as wind capacity and revenue expand across the EU (Datta & Acton, 2026).

Targeting decisions are driven by the probability and scale of monetisable outcomes rather than by symbolism, and the wind sector meets this criterion through several channels. Wind energy manufacturers, developers, and operators are increasingly large, well-capitalised organisations that meet the profile associated with "Big Game Hunting" targeting logic; the sector's dense ecosystem of maintenance providers, SCADA vendors, and engineering contractors creates a broad population of smaller, less mature organisations whose compromise can nonetheless provide a pathway into higher-value operator or manufacturer networks; and the reputational and regulatory sensitivity of the energy transition gives cybercrime operators additional leverage in double-extortion negotiations, since public disclosure of a compromise at a wind operator carries reputational stakes tied to national energy-policy commitments as well as ordinary commercial harm (Meurs et al., 2024).

The already-documented ransomware incidents affecting Deutsche Windtechnik, Nordex, and Vestas (4.3) show this logic has already materialised in the European wind sector, and the broader energy-sector cases involving HSE Slovenia and Electrica Group indicate the pattern is not confined to wind-specific entities. The technical playbook does not differ substantially from that used against other critical-infrastructure victims: initial access is

most commonly achieved through phishing, exploitation of exposed remote-access services, or the purchase of already-compromised credentials from initial-access brokers, and affiliates typically prioritise identifying and exfiltrating data with negotiation value, including engineering documentation, contracts, and personal data, before deploying encryption.

A distinguishing feature relevant to offshore wind, however, is that operators appear, to date, to have stopped short of directly compromising turbine-control environments: as discussed in 4.3, wind-sector victims have responded to ransomware primarily by isolating remote-monitoring links between enterprise IT and turbine-facing systems, rather than experiencing direct encryption of SCADA or turbine-control environments, suggesting current tooling remains optimised for IT-layer disruption rather than the more specialised intrusion techniques control logic would require, although this should be read as a present-day observation rather than a structural limitation.

Beyond the wind-sector-specific ransomware cases already discussed in 4.3, the clearest historical precedent for financially motivated cybercrime against energy infrastructure remains the May 2021 **Colonial Pipeline** incident in the United States, in which the **DarkSide** ransomware affiliate model forced the shutdown of a pipeline supplying roughly half the fuel consumed on the US East Coast after gaining access through a single reused VPN password (Lakshmanan, 2021). The case demonstrated both the disproportionate operational consequences a criminally motivated, non-targeted intrusion can produce in an energy-adjacent sector, and its capacity to generate contagion effects across related commodity and equity markets beyond the victim organisation itself (Goodell & Corbet, 2022).

The boundary between "pure" cybercrime and state-tolerated or state-adjacent criminal activity, discussed further in relation to hybrid actors in 5.4, is often difficult to draw with confidence in energy-sector cases: the 2022 Nordex incident, for instance, was linked in external reporting to Conti-affiliated actors. Overall, cybercrime operators should be assessed as the most consistently active and highest-likelihood adversary category for the European wind energy sector, given the combination of documented prior incidents, an increasingly professionalised RaaS ecosystem, and a sector-wide dependence on IT and remote-access infrastructure that provides ample opportunity for opportunistic and targeted intrusion alike.

Hacktivists

There is limited public evidence that hacktivists have been directly involved in cyber incidents affecting offshore wind farms; most publicly documented incidents involving the wind and wider energy sectors appear to fit other categories, including ransomware, state-linked espionage, destructive cyber operations, or collateral disruption linked to broader geopolitical campaigns. Even so, hacktivism remains a plausible threat scenario: the sector sits at the intersection of energy security, climate policy, maritime infrastructure,

critical national infrastructure, and geopolitical competition, a combination that makes offshore wind a highly visible and symbolically attractive target.

An attack against an offshore wind operator could be framed as opposition to a government's energy policy, a country's economic interests, or a company's role in a contested political issue, and in some cases attackers may invoke environmental narratives, claiming that offshore wind development harms marine ecosystems, coastal communities, or natural landscapes, a framing that in more extreme scenarios could overlap with eco-terrorism or sabotage aimed at disrupting activities perceived as environmentally harmful.

For these reasons, hacktivism should be treated as a credible but not yet well-established threat pattern for offshore wind farms. The strongest relevant example is the October 2024 DDoS wave against Cyprus (I-13), during which critical infrastructure and government services, including the Cyprus Telecommunications Authority (CYTA), the Cyprus Electricity Authority (EAC), and EKO Cyprus Limited, were targeted, and several pro-Palestinian hacker groups, most likely **LulzSec Black** and **Moroccan Soldiers**, claimed responsibility as retaliation for Cyprus' perceived support for Israel. Official Cypriot reporting did not publicly attribute the attacks or confirm the motive, so the case should be described as hacktivist-claimed rather than definitively hacktivist-attributed, and this ambiguity, between independent hacktivist activity and state-aligned operations that may echo, support, or amplify a state's interests, is a recurring feature of the category: the same attack may be presented publicly as activism while still serving broader geopolitical objectives.

The lesson for offshore wind is that symbolic value can be just as important as technical relevance when hacktivists choose targets: offshore wind represents national energy policy, climate transition goals, maritime activity, and major infrastructure investment, and a campaign against an operator could generate attention even if the technical impact is limited, since hacktivists often target what is visible and easy to publicise rather than what is most operationally central.

For offshore wind, the most realistic hacktivist techniques are likely to be relatively low-complexity but high-visibility: DDoS attacks against public websites or customer-facing portals, website defacement, data-leak claims, disruption of third-party service providers, and opportunistic abuse of exposed remote-access systems, aimed more at generating public attention and reputational pressure than at causing long-term operational damage. More capable or state-aligned hacktivist groups may attempt to go further, particularly where remote-access services, OT interfaces, or management systems are poorly secured; a joint advisory from the NSA, FBI, CISA, and partners warned that pro-Russia hacktivist groups have targeted critical infrastructure by exploiting inadequately secured remote access to OT control devices, demonstrating that hacktivist activity is not limited to public websites and can, under certain conditions, extend toward operational environments.

Historical precedent for cyberattacks on power grids by environmental extremists or anarchist groups remains limited; eco-terrorism and issue-driven sabotage have

traditionally favoured physical action such as arson, vandalism, and equipment tampering. The threat landscape is evolving, however, and intelligence and terrorism studies have noted a broader shift among some issue-driven groups toward digital infrastructure, including digitally networked mobilisation and the use of IT and OT systems to create wider disruption (Humpal, 2026).

Overall, hacktivism should not be overstated as a proven source of cyber incidents against offshore wind farms, since the public evidence base remains limited, but the sector's symbolic value, connection to national policy, and dependence on digital and remote systems make it a plausible target. For offshore wind operators, the main risk is likely to come from disruptive and reputationally damaging activity such as DDoS attacks, defacement, data-leak claims, and opportunistic targeting of exposed systems; the more serious risk is that politically motivated or state-aligned hacktivists may attempt to reach operational environments where remote-access controls are weak.

Hybrid & Information Operation Actors

Hybrid and information operations actors differ from the other adversary categories addressed in this chapter in that their objective is not necessarily to compromise, disable, or extort a wind energy organisation's systems directly, but to use disinformation, narrative manipulation, or ambiguous, below-threshold physical and cyber action to erode public support for the sector, complicate attribution, or advance broader strategic competition. As offshore wind expands, it becomes simultaneously a target for narrative attack and, through the undersea cabling and cross-border grid dependencies, a potential object of ambiguous physical interference consistent with wider hybrid-warfare patterns already observed elsewhere in European critical infrastructure.

Unlike cybercrime operators, these actors, whether state, state-aligned, or ideologically motivated non-state groups, are generally not seeking direct financial gain; their objectives are better understood as strategic: undermining public confidence in the energy transition, slowing the regulatory and investment momentum behind renewable deployment, or, in a maritime and infrastructure-sabotage context, signalling coercive intent without crossing a threshold that would justify an unambiguous military or diplomatic response. Marsili (2025) frames this as a form of "information control," in which state and non-state actors deploy disinformation, algorithmic amplification, and platform-level influence to shape the narratives that underpin public support, investment flows, and geopolitical partnerships around Europe's energy transition, identifying Russian-linked efforts to sow doubt over EU energy security as one recurring vector. This motivational logic is reinforced by a sustained pattern of leveraging energy dependency, infrastructure vulnerability, and information operations as complementary instruments of strategic pressure against European states rather than as isolated or opportunistic activity; because these campaigns operate below the threshold of open conflict, they are typically designed for plausible deniability, allowing a state sponsor to signal displeasure or extract leverage while avoiding the escalatory consequences of overt attribution.

Offshore wind farms are targeted, or made subject to narrative attack, less because of any unique technical vulnerability than because of their symbolic and strategic position within the broader energy transition. Wind energy is closely associated with EU climate policy and the European Green Deal, making it an attractive target for narratives that seek to undermine public confidence in the pace, cost, or reliability of the transition rather than in any single operator; this vulnerability is not marginal, as public-opinion research across the United States, United Kingdom, and Australia shows over a quarter of surveyed respondents agreed with at least half of a set of contrarian claims about wind farms, with agreement strongly predicted by a general conspiracist worldview and inversely predicted by pro-ecological attitudes (Winter et al., 2024), and similar dynamics have been documented at a more local level in Europe, where anti-wind Facebook communities in Denmark have served as effective mobilisers of local opposition to specific projects, blending legitimate local grievances with amplified narrative campaigns. The undersea and cross-border infrastructure on which offshore wind depends, including export cables and interconnectors, is targeted for a related but distinct reason: it sits within the same class of exposed, difficult-to-monitor undersea assets that has already been subject to ambiguous sabotage incidents in the Baltic Sea, where responsibility is difficult to attribute conclusively but where the strategic effect (cost imposition, disruption, and demonstration of reach) is achieved regardless of formal attribution.

Hybrid and information operations relevant to offshore wind fall into two broad, and increasingly interconnected, categories. The first is narrative and disinformation activity conducted primarily through social media and online platforms, including the amplification of misleading claims about the health, economic, or environmental effects of wind turbines, the promotion of "renewable delayism" narratives that exaggerate technical limitations to justify continued reliance on fossil fuels, and the targeted discrediting of public officials or companies associated with specific projects (Marsili, 2025); these campaigns typically require limited technical sophistication but benefit from algorithmic amplification, coordinated inauthentic activity, and, increasingly, generative-AI tooling capable of producing large volumes of persuasive content at low cost.

The second category is ambiguous physical or cyber-physical interference against shared infrastructure, most visibly illustrated by a series of anchor-dragging and suspected deliberate damage incidents affecting undersea cables and pipelines in the Baltic Sea since 2022, attributed with varying degrees of confidence to vessels linked to Russia's so-called shadow fleet; although these incidents have to date targeted telecommunications cables, gas pipelines, and power interconnectors rather than offshore wind export cables specifically, the technique, physical damage to poorly monitored undersea assets combined with ambiguous attribution, applies directly to the cabling on which offshore wind farms depend, and should be regarded as a directly transferable risk pattern rather than a hypothetical one (Miętkiewicz, 2025).

The clearest precedent for information operations directed against the credibility of the wind sector itself is the now well-documented, cross-national pattern of coordinated

misinformation about wind farms, shown by academic survey research to be a mainstream rather than fringe phenomenon, correlated with underlying conspiracist worldviews and associated with reduced support for pro-wind policy and greater willingness to protest against specific projects (Winter et al., 2024); related work on social media mobilisation against wind power in Denmark demonstrates that these dynamics translate into concrete, localised opposition to individual projects rather than remaining abstract online discourse (Borch et al., 2020).

For the infrastructure-sabotage dimension, the strongest precedents are the 2022 Nord Stream pipeline sabotage and the subsequent series of undersea cable and pipeline incidents in the Baltic Sea, including damage to the Baltic connector gas pipeline in 2023 and to telecommunications cables in the following years, which have prompted the European Commission and NATO to treat undersea critical-infrastructure protection as a priority hybrid-threat concern. As discussed in 5.3 in relation to the October 2024 Cyprus DDoS campaign, the boundary between hacktivist-claimed activity and state-aligned hybrid operations is frequently blurred; the same ambiguity applies to hybrid actors more broadly and is likely to remain a defining feature of the category rather than a temporary attribution gap. Overall, hybrid and information operations actors should be assessed as a growing-relevance threat to the European offshore wind sector: current evidence does not show wind-specific undersea cable sabotage, but the precedent base for both narrative attack on the sector's legitimacy and physical interference with shared undersea infrastructure is already substantial and directly applicable.

Figure 7 compares the four adversary categories assessed in this section. Two of the four, state-nexus intrusion sets and cybercrime operators, account for the incidents in which impact on European wind assets has been publicly documented since 2022; hacktivist and hybrid or information operations activity relevant to the sector has to date been directed at adjacent or shared infrastructure, or at the sector's public legitimacy, rather than at wind assets themselves.

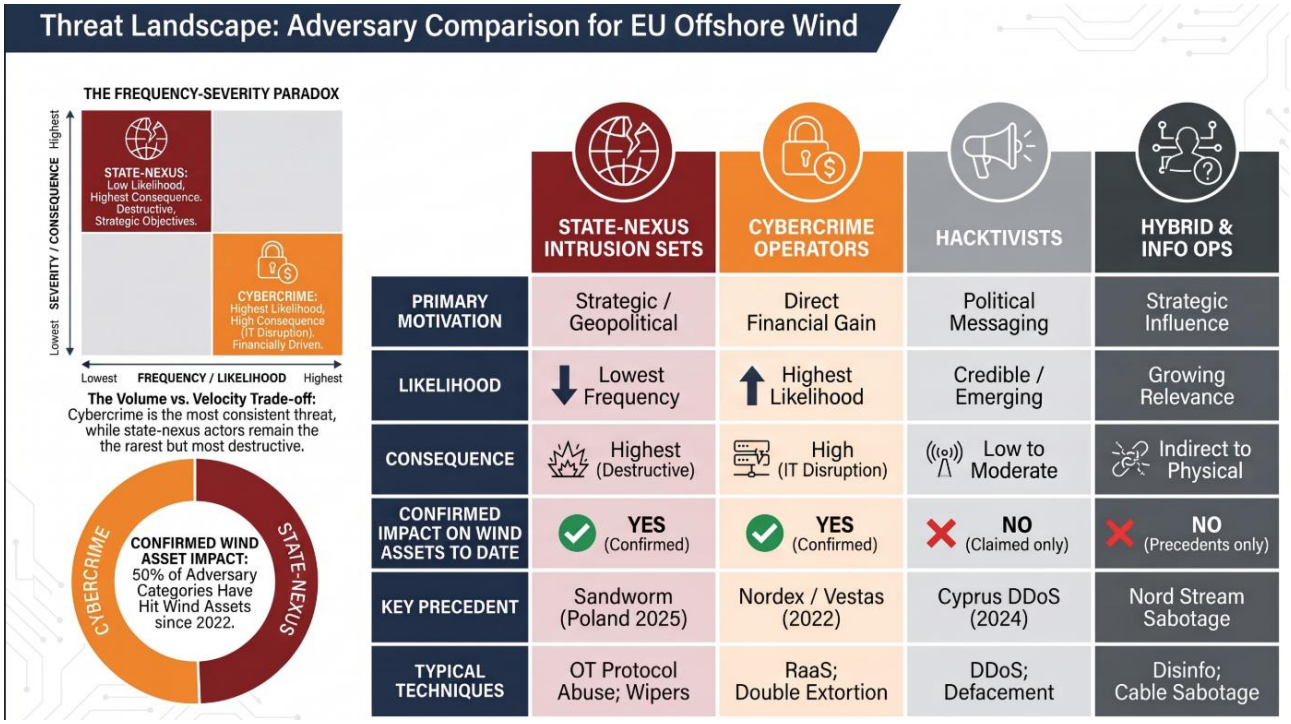

Figure 7: Adversary Comparison for Offshore Wind

10. Attack Surface & Supply Chain Dependencies

ICT Supply Chain of Offshore Wind

The ICT supply chain supporting offshore wind extends beyond the wind farm owner and spans six broad layers: hardware and embedded firmware in turbine controllers, protection relays, intelligent electronic devices and network equipment; the software estate, including SCADA and historian platforms, engineering toolchains, firmware images and their underlying third-party libraries; cloud and SaaS services used for condition monitoring, analytics and asset management; communications infrastructure, including fibre, satellite links and SD-WAN overlays; identity and remote-access services mediating OEM and contractor connectivity; and the engineering data exchanged across all of them. Delivery of these layers depends on a network of shipyards, marine contractors, engineering companies, equipment manufacturers, system integrators and service providers responsible for constructing, transporting, installing, commissioning, maintaining and upgrading offshore energy infrastructure. Because each of these layers is supplied and maintained outside the owner's direct control, the security posture of the asset is in practice the aggregate posture of its suppliers (Knack et al., 2024; Freeman et al., 2024). Cybersecurity risks arise throughout the engineering and maintenance lifecycle, where numerous organisations exchange technical data, software, configuration files and operational information required to deliver safe and efficient offshore operations.

Visibility into these layers is the principal gap. Owners routinely lack a component-level inventory of the software and firmware running in their own assets, which makes it difficult to determine exposure when a vulnerability is disclosed in a widely used library, protocol stack or remote-access product. In multi-vendor digital substations the problem is acute: intelligent electronic devices from several manufacturers share a common IEC 61850 configuration, and no single supplier holds a complete view of the resulting dependency graph. Structured approaches such as a substation bill of materials, which derives a machine-readable component inventory from the substation configuration description, offer a practical route to closing this gap (Yurrebaso et al., 2025). The Cyber Resilience Act's obligations on products with digital elements, discussed in Section 2.2.2, will make comparable component transparency a regulatory expectation rather than a discretionary practice.

Within this chain, shipyards and marine engineering contractors function as digital integration hubs rather than solely fabrication facilities. Modern offshore projects require the integration of electrical systems, propulsion and positioning equipment, cranes, automation systems, industrial control systems (ICS), SCADA interfaces, communications networks, navigation equipment, dynamic positioning (DP) systems, condition-monitoring platforms and remote diagnostics. During vessel construction, offshore platform fabrication, retrofit campaigns or maintenance periods, these systems are installed,

configured, tested and commissioned by multiple contractors working simultaneously within a shared digital environment.

The digital supply chain therefore includes not only turbine OEMs and electrical equipment manufacturers but also marine equipment suppliers, automation vendors, classification societies, subsea contractors, communications providers, software developers, cloud-service operators, logistics companies, testing laboratories and specialist maintenance organisations. Engineering documentation, 3D design models, PLC software, firmware packages, configuration files, commissioning procedures, calibration data and digital certificates are routinely exchanged between project participants, creating numerous trust relationships that must be appropriately managed.

Unlike fixed industrial facilities, offshore assets frequently undergo maintenance and modification while remaining operational. Shipyards supporting offshore wind projects regularly receive service operation vessels (SOVs), crew transfer vessels (CTVs), installation vessels, offshore substations and floating structures for scheduled maintenance, emergency repairs or life-extension programmes. These activities often require temporary connections to operational technology networks for diagnostics, software updates, equipment calibration, factory acceptance testing (FAT), harbour acceptance testing (HAT), commissioning support and performance verification. Consequently, maintenance periods may temporarily expand the cyber-attack surface through the introduction of engineering laptops, portable test equipment, removable media and vendor-specific diagnostic tools.

The increasing use of digital shipyard technologies further strengthens these interdependencies. Asset lifecycle management platforms, digital twins, predictive maintenance systems, remote inspection technologies, drones, autonomous survey vehicles and cloud-based engineering collaboration platforms have become integral to offshore maintenance activities. While these technologies improve efficiency and reduce offshore intervention costs, they also introduce additional dependencies on external software providers, cloud infrastructure and communications services whose disruption may affect project execution or operational availability.

A significant concern for marine contractors is the concentration of supply-chain risk. Offshore wind projects frequently standardise on common turbine platforms, automation systems, satellite communications providers, remote-access technologies and engineering software across multiple projects. A vulnerability affecting a widely deployed software platform, remote maintenance solution or cloud service may therefore simultaneously impact numerous vessels, offshore installations and maintenance providers operating across different regions. Such common-mode failures have the potential to delay maintenance campaigns, interrupt commissioning activities and reduce the availability of specialist engineering support during critical operational periods.

Cybersecurity governance should therefore extend across the full ICT supply chain and the complete engineering and maintenance lifecycle. Organisations should maintain comprehensive inventories of digital assets, engineering workstations, software versions,

temporary maintenance connections, portable diagnostic equipment and authorised supplier access. Procurement processes should incorporate cybersecurity requirements covering secure software development, vulnerability management, incident reporting, software provenance, privileged-access control and supplier security assurance. Emphasis should be placed on controlling temporary engineering access during refit and maintenance periods, ensuring that all modifications are validated, documented and independently verified before operational systems are returned to service.

Ultimately, resilient offshore supply chains depend on trusted collaboration between asset owners, shipyards, OEMs, marine contractors and specialist service providers. The objective is not to eliminate third-party involvement, which is fundamental to offshore operations, but to ensure that digital trust relationships remain transparent, controlled and recoverable throughout the operational lifecycle. This provides the foundation for the examination of third-party and vendor exposure presented in the following section.

Third-Party & Vendor Exposure

Third-party and vendor exposure is structurally high in offshore wind because the owner's operational capability depends on a broad ecosystem of specialised suppliers rather than on a single technology stack. The most visible dependency is the wind turbine OEM, which typically provides the generating units, turbine controllers, OEM SCADA, Power Plant Controller integration, remote monitoring, firmware/software support, major corrective maintenance and access to proprietary diagnostics. However, the wider exposure also includes network and SCADA device vendors, substation protection suppliers, electrical equipment manufacturers, telecommunications providers, condition-monitoring platforms and peripheral system vendors. In practice, an offshore wind farm's digital and operational perimeter includes not only turbines and substations, but also structural condition monitoring systems, CCTV and alarm networks, radar or bird-detection systems, underwater sonar or seabed-monitoring devices, protection relays, RTUs, AVRs, switchgear, power transformers, export and array cables, offshore and onshore substations, and the data gateways that connect these systems to owners, TSOs, traders, OEMs and cloud platforms.

This exposure is particularly pronounced during the first operational years, when many offshore wind farm owners rely on full-scope service and maintenance agreements with the turbine OEM, often covering availability commitments, scheduled and unscheduled maintenance, remote monitoring, software support and access to critical spare parts. This model reduces the owner's short-term operational burden and gives funders confidence that the OEM remains accountable for turbine performance, but it also concentrates operational knowledge, remote access, spare-parts availability and fault-resolution capability in one supplier relationship. The risk is not limited to the availability of physical components: if the OEM's SCADA platform, remote-access infrastructure, diagnostic tools, identity systems or service organisation are disrupted, the owner may lose visibility, troubleshooting capability or the ability to return turbines to service quickly, even where the turbines themselves remain technically healthy.

As offshore wind farms mature, owners often move gradually from a fully OEM-led model toward a more owner-controlled operating model, building internal spare-parts catalogues, warehouse and logistics processes, stock-management tools, component repair frameworks and alternative supplier arrangements for selected systems. This transition can reversions and dependency, but it also introduces new governance and cybersecurity requirements: the owner must maintain accurate asset and spare-parts data, secure procurement and inventory platforms, qualify alternative suppliers, track firmware and hardware versions, and ensure that replacement parts remain compatible with protection settings, SCADA mappings, communication protocols and grid-code requirements.

Wind turbine OEM exposure normally remains the highest because turbines and turbine SCADA are proprietary and because major components and control-system support are difficult to substitute; accordingly, owners commonly mitigate this through spare-part availability contracts, minimum stock obligations, agreed lead times, escalation procedures and contractual rights to technical documentation or post-termination support. For peripheral systems and electrical infrastructure, the exposure is more distributed but still material: compromise, insolvency or unavailability of a specialist vendor for CCTV, radar, sonar, CMS, relays, transformers, cables or gateways can delay restoration, reduce situational awareness, weaken physical security or create hidden dependencies that only become visible during an incident.

The survey findings reported in Section 3.2 corroborate this picture from the operators' own perspective. Every energy respondent reported supplier remote access into their environment, and every one identified OEM vendors as their primary systemic dependency risk. Third-party access is also the entry point they rank as most concerning, by a wide margin and more heavily than any other group in the sample. The exposure described above is therefore not only structural; it is recognised as the principal systemic risk by those who manage it daily.

Remote Access & Maintenance Channels

Remote access and maintenance channels are one of the most important attack-surface areas for an offshore wind farm owner because they connect geographically remote, safety-critical and revenue-generating assets to multiple external stakeholders. As described in Section 2.3, a modern offshore wind farm typically depends on VPNs, site-to-site tunnels, remote desktop tools, SD-WAN links, OEM firewalls, cloud collectors and industrial protocol gateways to support turbine monitoring, substation supervision, market dispatch, TSO telemetry exchange and owner/operator control-room activities. These channels are operationally necessary: offshore assets cannot be inspected or reset physically at short notice, and weather windows, vessel availability and specialist personnel constraints make remote diagnosis and intervention essential. However, the same channels also create privileged pathways into SCADA servers, historians, Power Plant Controllers, substation gateways, engineering workstations, CCTV/alarm systems, condition-monitoring platforms and vendor-managed services.

The highest-risk maintenance channels are usually those that combine privileged access, operational reach and third-party dependency. OEM remote access is especially sensitive where the OEM remains network administrator for the wind turbine segment under a full-scope agreement, because the OEM may retain persistent connectivity to turbine controllers, OEM SCADA, diagnostics tools and firmware/software support environments. Owner/operator VPN access is also sensitive because it may provide broad visibility across multiple segments for monitoring, reporting, administration and troubleshooting. Trader and TSO links are narrower in purpose, but they are operationally critical because they exchange telemetry and active-power or grid-related setpoints with the Power Plant Controller or substation gateways. Second-level SCADA and cloud monitoring platforms add another exposure layer by collecting real-time and historical data from OEM and substation systems and redistributing it through APIs, dashboards and reporting services. If any of these channels is compromised, misconfigured or deliberately disabled during incident containment, the owner may face loss of view, delayed fault diagnosis, inability to confirm plant status, degraded restoration capability, or uncertainty over whether commands and telemetry can be trusted.

For an offshore wind farm owner, the practical objective is not to eliminate remote access, but to make it controlled, segmented, attributable and recoverable. Maintenance access should be granted through approved paths only, with multi-factor authentication, named accounts, role-based permissions, least-privilege access, time-bound approvals, jump hosts or controlled access brokers, session logging, and clear separation between corporate IT, owner peripheral networks, OEM turbine networks, substation protection networks and auxiliary systems. Persistent vendor tunnels should be reviewed against operational need, and emergency access procedures should be tested before an incident occurs. The owner should also maintain an up-to-date inventory of all remote connections, protocols, accounts, certificates, firewall rules, cloud collectors and vendor support arrangements, including who can access which asset, from where, for what purpose and under which contractual authority. In cyber incident response, this inventory becomes operationally critical: it allows the owner to isolate risky paths without unnecessarily losing all visibility, to preserve trusted communication with the TSO and trader, and to restore maintenance access in a controlled sequence rather than reopening the entire digital perimeter under pressure.

11. Impact Analysis

Operational Disruption

Operational disruption is the most immediate and financially visible consequence of a cybersecurity event for a wind farm owner. In the operating model described in Section 2.3, production depends not only on turbines and substations, but also on SCADA visibility, OEM remote support, owner/operator VPN access, trader and TSO telemetry links, second-level monitoring platforms and cloud-connected auxiliary systems. A cyber incident does not need to take direct control of turbine PLCs to create material impact: loss of view, loss of remote control, forced network isolation, unavailable historian data, disabled dispatch interfaces, or delayed restoration after curtailment can all reduce generation, slow fault response and increase the duration of outages.

For a wind farm owner with approximately 1 GW of installed offshore wind capacity, the scale of this exposure is significant. Using an illustrative annual yield of approximately 3,743 MWh per installed MW, equivalent to around 10.3 MWh per MW per day and to a net capacity factor of approximately 43%, and a contracted-revenue range of €80–€120/MWh consistent with recent European offshore wind auction outcomes (Energy Institute, 2026; WindEurope, 2025b), the direct gross revenue at risk from unavailable generation is approximately €820–€1,230 per MW per day when rounded. For a 1 GW portfolio, a full-day outage would therefore place approximately €0.82–€1.23 million of gross revenue at risk. Table 3 sets out the corresponding exposure for one-day and three-day outages across a range of affected capacities.

Calculation basis: 3,743 MWh/MW/year ÷ 365 = approximately 10.3 MWh/MW/day. Revenue loss per MW per day = 10.3 MWh/MW/day × achieved or contracted price. At €80/MWh, this equals approximately €820/MW/day when rounded. At €120/MWh, this equals approximately €1,230/MW/day when rounded. Therefore, the gross revenue loss from a cyber-induced outage can be estimated as: **affected MW × outage days × €820–€1,230/MW/day**. For 1 GW of installed offshore wind capacity, this equals approximately **€0.82–€1.23 million per day** under a full-production-loss scenario. The yield assumption is an illustrative planning figure equivalent to a net capacity factor of approximately 43%, within the performance range of modern European fixed-bottom offshore wind. The €80–€120/MWh band is anchored on recent European offshore wind auction outcomes, including the UK AR7 clearing prices of £89.49–£91.20/MWh (2024 prices) and the December 2025 Polish CfD awards at approximately €113–€117/MWh (Energy Institute, 2026; WindEurope, 2025b). These figures should be treated as indicative because actual losses depend on wind resource during the outage, support scheme, market price, curtailment status, imbalance exposure, asset-specific tariff and whether the affected plant is under Feed-in Tariff (FiT), Feed-in Premium (FiP), Power Purchase Agreement (PPA) or merchant arrangements.

Table 3: Financial impact from OWF operational disruption

Affected capacity	1-day outage	3-day outage	7-day outage
10 MW	€8.2k–€12.3k	€24.6k–€36.9k	€57.4k–€86.1k
100 MW	€82k–€123k	€246k–€369k	€574k–€861k
1 GW portfolio	€0.82m–€1.23m	€2.46m–€3.69m	€5.74m–€8.61m

For floating offshore wind farms, the financial exposure can be materially higher because contracted revenues may reach approximately €150–€250/MWh, a band consistent with the £216.46/MWh floating offshore wind strike price awarded in the UK AR7 round and with published floating-wind LCOE mapping for the European Atlantic (Energy Institute, 2026; Martinez & Iglesias, 2022). Under the same yield assumption, this would correspond to roughly €1,540–€2,570 per unavailable MW-day, meaning that the revenue impact of a full outage can be almost double, or more, compared with the fixed-bottom offshore wind revenue range used above.

The total business impact would normally exceed the lost energy revenue shown above. First, if SCADA or second-level monitoring is unavailable, operators may need to run assets in a degraded mode, increasing reliance on local teams and OEM support while reducing the speed of fault detection and restart. Second, if market, trader or TSO interfaces are affected, the owner may face imbalance exposure, inability to follow dispatch instructions, or delayed response to curtailment and restoration signals. Third, cyber containment actions may intentionally disconnect VPNs, OEM links, cloud collectors or remote desktop channels, protecting OT systems but extending downtime and delaying diagnostics. Fourth, if the event affects multiple sites through a common supplier, identity platform or SD-WAN / remote-access layer, losses can scale rapidly across the portfolio rather than remaining confined to one wind farm.

Operational disruption should therefore be assessed in MW-days rather than only in incident duration. A short outage affecting a large share of the portfolio may be more financially material than a longer outage at a small site. For a wind farm owner, a practical risk metric is **gross revenue at risk per unavailable MW-day**, supported by scenario bands for 10 MW, 100 MW and full-portfolio disruption. This metric can be used in cyber range exercises, incident response playbooks and business continuity planning to translate technical events—such as loss of VPN access, ransomware containment, SCADA unavailability, telecommunications outage or supplier compromise—into operational and financial consequences that management can prioritise.

Grid Stability & Cross-border Implications

The 9 August 2019 Great Britain power disruption provides a useful reference case for assessing the grid-stability implications of a sudden offshore wind farm outage. Public investigations by Ofgem, National Grid ESO and the UK Energy Emergencies Executive

Committee found that the near-simultaneous loss of two large generating units, including Hornsea One, caused a rapid frequency excursion and triggered Low Frequency Demand Disconnection (LFDD). More than one million customers were affected, with direct electricity supply restored within a short period but with wider secondary impacts, particularly to rail and other essential services, lasting significantly longer (Ofgem, 2020; E3C, 2020; National Grid ESO, 2019). The relevance of the case is not the initiating event, but the system behaviour that followed: a large, sudden generation loss can move very quickly from an asset-level disturbance to a national grid-resilience event.

For offshore wind cybersecurity, this case demonstrates that the operational impact of an outage is determined by electrical system dynamics rather than by the technical origin of the disturbance. A cyberattack that causes a large offshore wind farm to disconnect, rapidly reduce active power output, fail to follow dispatch instructions, or lose plant-controller coordination could create the same system challenge as any other sudden generation loss: frequency falls because demand temporarily exceeds available generation, automatic frequency response is called upon, and if the imbalance is too large or too fast, protection schemes may disconnect demand to prevent wider instability. In highly decarbonised systems with increasing inverter-based resources, the speed of response, accuracy of telemetry, performance of grid-code functions and availability of reserve become even more important because system inertia and conventional synchronous response may be lower than in historical generation mixes.

A cyber-induced outage at an offshore wind farm could affect grid stability through several pathways. First, compromise of the Power Plant Controller or SCADA-to-controller interface could cause an abrupt loss of export or an uncontrolled ramp-down. Second, manipulation or loss of telemetry could reduce the transmission system operator's ability to assess real-time output, available reserves, voltage conditions and restoration status. Third, attacks on communications links between the offshore substation, onshore control centre, market operator, TSO and OEM support functions could delay corrective action even where the turbines and electrical plant remain technically healthy. Fourth, a coordinated attack across several projects that share the same OEM platform, telecommunications provider, remote-access architecture or cloud monitoring service could create a correlated loss of generation that is more severe than the outage of a single asset.

The cross-border dimension is also important. Offshore wind farms are increasingly connected into meshed transmission zones, offshore hubs, interconnectors and market-coupled regions. A large offshore outage in one bidding zone can influence balancing requirements, reserve activation, cross-border flows and interconnector schedules in neighbouring systems. If the affected system suddenly imports more energy or reduces expected exports, adjacent TSOs may need to rebalance their own networks while respecting congestion limits and frequency-stability requirements. Where offshore wind output is forecast and traded day-ahead or intraday, an unplanned cyber-related loss may also create imbalance exposure for market participants and increase reliance on balancing

energy from neighbouring countries. In a stressed system, the result could be price volatility, emergency redispatch, constraint management, or curtailment of other generation to keep the network within secure operating limits.

The Hornsea One case supports a broader lesson for offshore wind cybersecurity: cyber resilience must be assessed not only at the level of confidentiality, malware containment or turbine availability, but also at the level of power-system stability. The most serious scenario is not necessarily permanent equipment damage; it may be a short, sudden and poorly coordinated loss of a large volume of generation at a moment when reserve margins, interconnector flows, weather conditions or network constraints leave little room for error. A realistic cyber scenario should therefore test whether the operator and TSO can maintain trusted telemetry, confirm the true state of the plant, execute safe ramping or disconnection, coordinate restoration, and communicate clearly with market, grid and emergency stakeholders under degraded digital conditions.

For this reason, cyberattacks on offshore wind farms should be treated as potential cross-border grid events when they affect large capacity blocks, common supplier platforms, offshore substations, plant controllers, or communications channels used for dispatch and balancing. Preparedness should include joint operator-TSO exercises, validation of frequency-response and fault-ride-through settings, secure fallback communication procedures, independent verification of plant output, and playbooks for controlled restoration after digital isolation. The objective is to prevent a cyber incident from becoming a cascading power-system event, and to ensure that if generation is lost, the loss is visible, bounded, communicated and recovered in a way that protects both national and interconnected European grid stability.

Safety & Environmental Impact

Offshore wind farms integrate information technology (IT), operational technology (OT) and cyber-physical processes across turbines, substations, communications, control centres, maintenance systems and supplier interfaces. Safety and environmental consequences arise through the operational function which may be affected by a cyber incident. AENAON's scope includes supervisory control and data acquisition (SCADA)/ industrial control systems (ICS), attack vectors, turbine and substation disruption, cyber-range testing and sector-specific preparedness. OT and wind-specific guidance likewise require security to account for performance, reliability and safety, supported by coordinated protection, detection, response and recovery (NIST, 2023; U.S. Department of Energy, 2020).

This section therefore translates the threat descriptions in Sections 4-6 into pathways with personnel and safe-work impacts, environmental and asset-integrity impacts, and offshore-specific aggravating factors. MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) for ICS[3] identifies loss or manipulation of view and control,

[3] MITRE ATT&CK for ICS – Impact (Tactic TA0105): https://attack.mitre.org/tactics/TA0105/

loss of protection or safety, damage to property and loss of availability as relevant impact patterns. Environmental impact is treated as conditional and secondary, where abnormal operation, damaged equipment, impaired protection, or delayed containment produces a physical consequence (Kulev & Sill Torres, 2022; CISA, 2022).

Cyber-to-physical impact pathways

Remote access and engineering workstations. Compromise can alter configurations or undermine diagnostics and restoration workflows (Sections 4.5, 4.6 and 6.3). Safety risk arises when operators or field crews plan work from untrusted asset, isolation or configuration data. Wind-specific research identifies malicious parameter manipulation as a route to excessive mechanical loads and component damage (Kulev & Sill Torres, 2022). Offshore verification, rollback and specialist intervention may then be delayed by weather windows, vessel availability and original equipment manufacturer (OEM) support.

Telemetry, alarms and condition-monitoring data. Manipulated or unavailable data can create a false 'normal' state, suppress alarms or present conflicting information. This can undermine work authorisation, isolation confirmation, fault diagnosis and restart decisions. Loss or manipulation of view is a recognised ICS impact pattern. Delayed detection of vibration, overheating, brake, pitch, converter or electrical anomalies can extend abnormal operation and increase component damage.

Communication and remote-control loss. Denial-of-service or destructive activity can isolate distributed assets without directly compromising turbine logic (Sections 4.7 and 5.1). During the 2022 KA-SAT incident, remote monitoring and control were reportedly lost for approximately 5,800 Enercon turbines while the turbines continued to operate automatically (Viasat, 2022; Reuters/Euronews, 2022). This illustrates loss of view and remote control rather than confirmed physical damage. Safety impact arises through reduced situational awareness and coordination; operational and conditional environmental impact arises if fault containment is delayed or additional offshore mobilisation is required.

Substation automation, protection and safety functions. Interference with relays, breaker-control interfaces, SCADA/ human-machine interfaces (HMIs) or safety functions can create unsafe switching or isolation assumptions, unexpected equipment states, loss of protection, or false assurance that a safe shutdown remains available. The 2015 Ukraine grid attack and Cybersecurity and Infrastructure Security Agency (CISA) 's TRITON reporting provide adjacent-sector precedents for substation disruption and compromise of safety systems[4] (CISA, 2022). For offshore wind, the consequences could include equipment damage, prolonged unavailability and increased risk to personnel, with on-site inspection and specialist revalidation required before control and protection states can be trusted.

OEM, operator and supply-chain support disruption. Ransomware or supplier compromise may not reach turbine-control systems directly, but it can disrupt

[4] MITRE ATT&CK, 2015 Ukraine Electric Power Attack (Campaign C0028): https://attack.mitre.org/campaigns/C0028/

maintenance planning, remote support, spare-part logistics, software and firmware assurance, and access to proprietary diagnostics. During its 2022 incident, Nordex shut down various IT systems and disabled remote access from its IT infrastructure to turbines under contract as a safeguard (Nordex, 2022). This increases uncertainty during troubleshooting and restoration and can create correlated disruption where several farms depend on a common OEM or platform. AENAON recognises these supply-chain and cascading dependencies, as discussed in Sections 6.2 and 9.3.

Degraded conditions, severe weather and active maintenance. Timing can materially change consequence severity. Loss of communication or trustworthy asset status during active work, severe weather, emergency response or a pre-existing equipment fault can increase risk to technicians, vessel crews and control-room staff. High-impact, low-probability research highlights cascading or 'snowball' effects at offshore-wind-farm scale (Kulev & Sill Torres, 2022). Environmental or asset-integrity consequences are most credible where abnormal operation persists while access, verification or containment is constrained.

Impact prioritisation

Higher analytical weight should be given to scenarios that create a credible path to loss or manipulation of view, control, protection or safety; coincide with active maintenance or degraded weather; remove independent means of verification; affect shared supplier or communication infrastructure; or require offshore access for recovery (NIST, 2023; Kulev & Sill Torres, 2022). Severity should not be inferred from the threat label alone: a simple communications outage can become safety-significant during offshore intervention, while a sophisticated intrusion may have limited physical consequence if independent protection and trusted fallback communications remain available.

Implications for AENAON preparedness

AENAON can represent these pathways safely through cyber-range and digital-twin-based exercises. Virtualised or emulated IT/OT components, representative network segments and simulated SCADA/ICS assets can reproduce false or degraded telemetry, blocked commands, manipulated setpoints, substation-state changes, communication failures and delayed maintenance decisions (AENAON Consortium, 2026).

Within Section 7.3, these should be used as impact-evaluation criteria rather than as a second recommendations section. Exercises should test whether participants can establish a trustworthy plant state, verify isolation and protection status, distinguish cyber compromise from equipment failure, coordinate with offshore and grid stakeholders, and move to a controlled safe state under degraded communications. Detailed exercise recommendations appear in Section 9.2.

The approach is consistent with ISO/IEC 27001 and ISO/IEC 27005 for security management and risk treatment, IEC 62443 for industrial automation and control-system security, and the NIS2 Directive, requirements for risk management, incident handling,

continuity, supply-chain security, access control and training[5]. Relevant offshore verification and cyber-resilience context is also provided by DNV-ST-0262, DNV-SE-0263 and DNV-RP-0496[6].

This perspective should be carried into AENAON requirements, cyber-range content, digital-twin models and pilot evaluation criteria. Its contribution is to make the cyber-to-physical escalation path explicit: which dependency is affected, which safety decision becomes unreliable, which offshore conditions worsen the consequence, and what evidence is required before safe recovery.

Reputational & Economic Impact

Reputational and economic impact is not a discrete threat category in the way that ransomware or DDoS are, rather, it is a cross-cutting consequence that follows from the threats described throughout Section 4 and the adversary behaviours described in Section 5. It nonetheless merits separate treatment because reputational and financial harm frequently represents the primary, and sometimes the only, materially significant consequence of a cyber incident affecting a wind energy organisation, particularly where the incident is contained to enterprise IT and does not reach turbine-control environments. For offshore wind, this dimension of impact interacts closely with the sector's exposure to public scrutiny as a flagship component of the European Green Deal and national energy-security strategy, discussed in Section 2.1, meaning that reputational harm arising from a cyber incident can extend beyond the affected company to the broader credibility of the energy transition.

Cybersecurity incidents affecting wind-sector organisations generate reputational harm through several distinct but related channels. Where an incident involves the exposure or theft of personal, commercial, or engineering data, as in the 2021 Vestas case discussed in Section 4.3, the resulting disclosure obligations and media coverage can damage stakeholder trust independently of any operational disruption. Research on the public consequences of cybersecurity incidents shows that public reaction is shaped less by the technical severity of an incident than by the credibility of the source reporting it and the perceived adequacy of the affected organisation's response (de Lemos & Ignaczak, 2023). This is consistent with broader findings that a company's post-incident communication strategy, for example whether it issues an apology or instead frames the incident as unavoidable, can itself materially affect investor and public perception, sometimes independently of the severity of the underlying breach (Masuch et al., 2022).

For offshore wind specifically, reputational risk is compounded by the sector's political visibility. Because offshore wind operators are widely understood as instruments of national climate and energy-security policy, an incident affecting a major operator or manufacturer, such as the ransomware cases affecting Deutsche Windtechnik, Nordex,

[5] ISO/IEC 27001:2022 and ISO/IEC 27005:2022, International Organization for Standardization; IEC 62443 series, International Electrotechnical Commission.
[6] DNV-ST-0262, DNV-SE-0263 and DNV-RP-0496 – offshore-wind standards, DNV (2016).

and Vestas described in Section 4.3, can be framed publicly as evidence of wider vulnerability in the renewable-energy transition rather than as an isolated corporate security failure. This dynamic increases the reputational stakes of any individual incident and gives cybercrime and hybrid actors alike, as discussed in Sections 5.2 and 5.4, additional leverage in extortion negotiations or narrative campaigns that reference the incident.

Beyond reputational harm, cybersecurity incidents impose measurable financial costs on affected organisations. Event-study research across large samples of publicly disclosed cyberattacks consistently finds a statistically significant negative effect on the market value of the affected firm around the disclosure date, although the magnitude reported varies considerably between studies, from around one percent of market value in early research (Goel & Shawky, 2009) to an average loss of over 300 million US dollars per incident across a larger and more recent sample of 776 cyberattacks between 2012 and 2022 (Muktadir-Al-Mukit & Ali, 2025). A meta-analysis spanning 63 studies and more than 20,000 disclosed incidents confirms that this negative market reaction is a robust and replicated finding, while noting that its size depends on factors including the type of breach, the sector involved, and the size of the affected firm (Ebrahimi & Eshghi, 2022).

The energy sector carries relevance for this dynamic because of its role in wider commodity and financial markets. The 2021 Colonial Pipeline ransomware attack demonstrated that a cyber incident affecting a single energy company can generate measurable price reactions and volatility across related energy commodity markets, prompting calls for regulators to treat certain energy firms as systemically important for the purposes of cyber-risk oversight (Goodell & Corbet, 2022; Janvrin et al., 2026). Sector-specific reviews of the economic impact of cybersecurity incidents on energy infrastructure similarly conclude that costs extend well beyond direct incident-response and recovery expenditure to include downtime, regulatory exposure, insurance costs, and long-term reputational drag on company performance (Venkatachary et al., 2017; Venkatachary et al., 2024).

Reputational and economic impact should be assessed as highly relevant to the EU offshore wind sector, both because the financial-market dynamics identified in the literature apply directly to publicly listed European turbine manufacturers, developers, and service providers, and because the sector's political salience under the European Green Deal and REPowerEU framework, discussed in Section 2.1, means that reputational harm from a cyber incident carries policy-level as well as commercial consequences. The already-documented cases affecting Deutsche Windtechnik, Nordex, and Vestas indicate that this exposure is not theoretical; each incident generated significant media coverage and, in the Vestas case, direct data-protection and disclosure obligations under GDPR. Because reputational and economic consequences frequently persist even where technical containment is successful, as in each of the wind-sector cases where operators isolated turbine-facing systems before encryption could spread, this impact category should be treated as a near-certain consequence of any future incident affecting the sector, rather than as a residual or secondary risk.

12. Outlook (12-24 months)

Expected Evolution of Threat Types

Over the next 12–24 months, the threat landscape for offshore wind farms is expected to evolve through the convergence of financially motivated cybercrime, destructive activity affecting OT-connected environments, dependency disruption, and increased targeting of remote monitoring and control pathways. The outlook does not suggest that offshore wind farms will face a wholly distinct set of cyber threats from the wider energy sector. Rather, the distinctive risk arises from how common threat types interact with offshore wind's operational model: geographically distributed assets, constrained physical access, continuous reliance on remote connectivity, multi-vendor maintenance arrangements, and increasing IT/OT integration.

Destructive cyber activity affecting OT-connected renewable energy environments is expected to remain a high-impact concern, particularly where attackers can disrupt monitoring, remote control or communications without necessarily halting generation. The late-2025 attacks analysed by CERT Polska illustrate this pattern; renewable-energy and combined heat-and-power environments were affected through destructive activity against exposed and weakly configured devices, leading to disruption of communications, monitoring and remote-control capabilities while generation continued (CERT Polska, 2026). For offshore wind, this is especially relevant because operational impact may arise not only from physical damage or turbine shutdown, but also from loss of visibility, delayed restoration, impaired coordination with grid operators, or reduced ability to perform remote diagnostics.

Ransomware is also expected to remain one of the most relevant threat types for wind-sector stakeholders, but its impact is likely to continue concentrating on enterprise IT, remote-support environments, data repositories and service coordination rather than on direct turbine-control compromise. Financially motivated actors are expected to continue using double-extortion models, combining encryption with data theft and public-leak pressure to increase leverage over operators, OEMs and maintenance providers (ENISA, 2024). This outlook is consistent with the incident patterns already discussed in this report, including ransomware cases affecting Vestas, Nordex, Deutsche Windtechnik, HSE Slovenia (Slovenske Elektrarne / HSE., 2023) and Electrica Group, where operational strain arose through business-system disruption, defensive isolation, reduced remote support or data exposure, even where core generation systems reportedly remained operational.

Targeting of SCADA, remote monitoring and control environments is likely to become more operationally significant, even if publicly confirmed wind-sector incidents remain limited. Wind-farm SCADA systems are exposed to risks arising from decentralised deployments, remote access, insecure or legacy communication protocols, vendor-managed infrastructure and Industry 4.0 integration (Sabev et al., 2021). This does not

mean that direct compromise of turbine control logic is expected to become common in the near term. However, the increasing dependence of offshore wind operations on SCADA visibility, second-level monitoring platforms, vendor access and telemetry exchange means that compromise of adjacent systems may be sufficient to create material operational consequences. The highest-impact scenarios therefore remain those where attackers move from IT or remote-access pathways toward environments that influence monitoring, command execution, protection systems or operational decision-making.

Availability attacks, including DDoS and perimeter denial-of-service activity, are expected to remain relevant because offshore wind operations depend on continuous communication between offshore assets, onshore control rooms, OEM platforms, transmission-system operators and market-facing stakeholders. The sPower incident, analysed in wind-sector attack-surface literature, demonstrated that disruption of internet-facing network infrastructure can sever visibility to renewable-energy assets without requiring specialised OT malware (Freeman et al., 2024). For offshore wind, similar disruption could affect situational awareness, monitoring continuity, remote maintenance coordination and grid-facing communication. DDoS should therefore be treated not only as a website-availability issue, but also as a potential loss-of-view or loss-of-coordination risk when supporting telecommunications or remote-access pathways are affected.

Integrity-oriented attacks, including manipulation of telemetry, false-command scenarios and abuse of legitimate credentials, are likely to remain lower-frequency but high-consequence concerns. The U.S. Department of Energy's wind cybersecurity roadmap identifies compromise of SCADA and plant control systems, communications manipulation, false-command or false-data attacks, remote-access abuse and supply-chain compromise as key threat scenarios for wind energy systems (Sanghvi et al., 2020). These scenarios are particularly relevant to offshore wind because operational decisions depend on trustworthy telemetry, coordinated dispatch, protection-system status, environmental monitoring and remote instructions. Even where attackers do not cause immediate physical damage, manipulated data or unauthorised commands could undermine operator confidence, delay response, trigger unnecessary shutdowns or complicate grid coordination.

Overall, the expected evolution of threat types suggests that offshore wind cybersecurity should not focus narrowly on direct turbine compromise. The more plausible near-term pattern is a combination of enterprise compromise, remote-access abuse, supplier-side disruption, data theft, loss of visibility, and selective destructive activity against exposed OT-connected or communications infrastructure. This reinforces the need for preparedness services that can test realistic scenarios across IT, OT, supplier, telecommunications and operational decision-making layers, rather than treating offshore wind cyber risk as a purely technical control-system problem.

Geopolitical Risk Drivers

Geopolitical risk is expected to remain a central driver of the offshore wind cyber threat landscape over the next 12–24 months. Offshore wind farms are not only energy assets; they are also strategic infrastructure linked to European energy security, decarbonisation, maritime security, cross-border electricity flows, and industrial supply chains. As a result, **the sector may be exposed to cyber operations, hybrid pressure, espionage, information operations and collateral effects from wider geopolitical conflicts, even where wind farms are not the initial or primary target.**

The most direct precedent is the cyberattack against Viasat's KA-SAT network at the start of Russia's full-scale invasion of Ukraine. The operation was publicly attributed by the UK and international allies to Russia and demonstrated how cyber operations in a regional conflict can generate wider European effects through commercial communications infrastructure (NCSC, 2022). For the wind sector, the relevance was concrete: the disruption affected satellite-based connectivity used for remote monitoring and control of more than 5,800 Enercon wind turbines in Germany, illustrating how a conflict-driven operation against a communications provider can impair visibility and remote operational capability across distributed renewable-energy assets (Knack et al., 2024). Similar spillover risks are likely to remain relevant where offshore wind farms depend on satellite links, telecommunications providers, remote-access platforms, or cross-border digital services that may be targeted for reasons unrelated to the wind sector itself.

Maritime hybrid threats are also expected to increase in relevance. Offshore wind farms depend on subsea export cables, offshore substations, interconnectors, telecommunications links, port infrastructure, maintenance vessels and maritime logistics. These dependencies overlap with the wider category of critical maritime infrastructure addressed in the revised EU Maritime Security Strategy and its action plan (Council of the European Union, 2023). The launch of NATO's Baltic Sentry activity in 2025, intended to strengthen the protection of critical infrastructure in the Baltic Sea following growing concern around undersea infrastructure security, further illustrates that cable, pipeline and seabed-infrastructure protection has become a strategic priority for European and allied security policy (NATO, 2025). For offshore wind, the key implication is that cyber risk cannot be separated from physical and maritime exposure; disruption to subsea cables, communications links, or offshore logistics may have cyber-operational consequences even where the initiating event is physical or ambiguous (Geri, 2024).

Strategic espionage against maritime, offshore-energy and supply-chain actors is likely to remain another important geopolitical driver. Campaigns such as the TA423 / Red Ladon activity documented against organisations connected to offshore energy production in the South China Sea show how state-linked actors may target offshore energy and maritime supply chains for credential theft, intelligence collection and long-term access (Raggi and Scenarelli, 2022). Similarly, the PoetRAT campaign documented by Cisco Talos showed interest in SCADA systems, including wind-turbine-related environments, in the context of targeted activity against Azerbaijani public and private-

sector organisations (Cisco Talos, 2020). These cases are not direct evidence of ongoing attacks against European offshore wind farms. However, they are relevant indicators of adversary interest in offshore energy, SCADA-adjacent environments, engineering documentation, and supply-chain relationships that could support future disruption, coercion or intelligence preparation.

State-nexus pre-positioning in critical infrastructure is also expected to shape the threat outlook. Recent joint advisories on People's Republic of China (PRC) state-sponsored activity, including Volt Typhoon, describe a pattern in which actors obtain and maintain persistent access to critical infrastructure using compromised edge devices, valid credentials, living-off-the-land techniques and stealthy lateral movement (CISA, 2024). This pattern should not be read as wind-specific evidence. Its relevance to offshore wind lies in the operating model of the sector: remote access, distributed assets, OEM and contractor connectivity, telecommunications dependencies and cloud-connected monitoring platforms create pathways where persistent access could remain undetected for extended periods. In a geopolitical crisis, such access could support disruption, intelligence collection, coercive signalling, or preparation for later destructive action.

Hybrid physical-cyber risks are also expected to become more prominent as offshore wind expands into increasingly complex maritime environments. Recent literature on the security of onshore and offshore wind farms in the context of war or terrorism highlights that offshore assets, particularly floating turbines, can be exposed through cables, substations, mooring systems and other hard-to-monitor components (Ivanov and Poita, 2025). These risks should not be treated as purely kinetic or purely cyber. A cyber incident that degrades monitoring, disables alarms, manipulates telemetry or disrupts maintenance coordination could amplify the impact of physical sabotage; conversely, physical damage to communications or power-export infrastructure could generate cyber-operational effects by reducing visibility, complicating restoration and forcing operators into degraded modes of operation.

Overall, the geopolitical outlook suggests that offshore wind operators should prepare for threat scenarios that combine direct cyber compromise with dependency disruption, maritime ambiguity, intelligence collection and narrative pressure. The most plausible near-term geopolitical risk is not a single large-scale cyberattack directly disabling turbines, but a sequence of events in which communications infrastructure, supplier access, remote monitoring, port logistics, subsea infrastructure or information integrity are disrupted in ways that affect operational confidence and resilience. This reinforces the need for preparedness exercises that test compound scenarios, including satellite or telecom disruption, supplier credential compromise, undersea cable damage, degraded SCADA visibility, and cross-border coordination under uncertain attribution.

Emerging Technical Risks

Emerging technical risks in the next 12–24 months should be understood primarily as **risk amplifiers** rather than wholly new threat categories. The core threats identified earlier in

this report - ransomware, supply-chain compromise, OT/ICS targeting, credential abuse, DDoS and AI-enabled threats - are expected to remain relevant. What is changing is the speed, scale and complexity with which these threats can interact with offshore wind's digital architecture, including remote-access pathways, vendor-managed environments, cloud-connected monitoring platforms, industrial controllers, engineering workstations and cross-border data flows.

AI-augmented cyber operations are likely to increase the speed and quality of adversary reconnaissance, vulnerability discovery and social engineering. Recent security-industry analysis warns that AI-driven vulnerability discovery and exploit development can compress defender timelines, making it harder for organisations to rely on slow manual triage and traditional patch-management cycles (Cloud Security Alliance et al., 2026). In the offshore wind context, the main near-term concern is not necessarily autonomous AI malware targeting turbines directly. Rather, AI is more likely to enhance existing attack paths: generating convincing multilingual phishing lures for engineering and operations personnel, automating discovery of exposed remote services, producing tailored pretexts for supplier impersonation, and supporting disinformation campaigns designed to undermine confidence in renewable-energy infrastructure. This outlook is consistent with the AI-enabled threat discussion earlier in this report, which treats AI as a cross-cutting capability uplift across the attack lifecycle rather than a standalone attack category.

Two consequences of that uplift are likely to become visible within the outlook window. The first concerns patch windows. As set out in Section 4.8, the interval between disclosure of a vulnerability and its first exploitation has compressed from years to hours, and AI-assisted exploit generation is the principal driver. Offshore wind operates on the wrong side of that compression: maintenance windows are limited, patching carries operational risk, and legacy equipment is widespread. Over the next 12–24 months the practical question for operators shifts from how quickly they can patch to what compensating controls hold while they cannot — segmentation, brokered and time-bounded remote access, and monitoring capable of detecting exploitation of a vulnerability that has not yet been remediated.

The second concerns autonomous agents in the supply chain. The first real-world attack executed end to end by an autonomous AI agent system, disclosed in July 2026 and described in Section 4.8 (OpenAI, 2026), establishes a category rather than a precedent: AI systems operated by vendors, OEMs or service providers may act as unintended attack vectors into the environments they connect to. Given that offshore wind depends on OEM remote access as a condition of operation, supplier assurance over the next two years should extend to how partners deploy and contain AI systems that touch operational infrastructure, not only to their conventional security posture.

Supply-chain and third-party platform compromise is expected to remain one of the most technically significant risks for offshore wind operators. The sector's operational model depends on trusted connectivity between owners, OEMs, maintenance providers,

telecommunications providers, cloud platforms, second-level SCADA services and market/grid stakeholders. Cross-sector incidents demonstrate how trusted service platforms can be weaponised at scale: the Kaseya VSA incident showed how compromise of a remote-management platform used by managed service providers can cascade to downstream customers (CISA, 2021), while Hitachi Energy's GoAnywhere incident illustrated how compromise of a third-party managed file-transfer provider can expose data held by an energy-sector technology supplier (Hitachi Energy, 2023). These examples are not offshore-wind-specific incidents, but they are technically relevant because offshore wind relies on similar trust relationships, remote support models and third-party digital services. For that reason, the boundary between "operator risk" and "supplier risk" is expected to become increasingly difficult to maintain in practice.

The technical complexity of offshore wind environments is also likely to increase as operators integrate more advanced monitoring, analytics and digital-twin capabilities. Such capabilities can improve resilience when properly governed, and the offshore-wind cyber-resilience literature identifies AI-enabled intrusion detection, anomaly detection, digital twins and predictive-maintenance approaches as promising defensive measures (Knack et al., 2024). However, these same developments also enlarge the dependency surface. Cloud-connected monitoring platforms, data collectors, APIs, operational historians, vendor portals and digital-twin interfaces create additional points where data integrity, access control, model trustworthiness and supplier assurance must be managed. The expected technical risk is therefore not simply that new tools introduce vulnerabilities, but that the overall system becomes harder to understand, test, segment and recover when multiple digital services participate in operational decision-making.

Advanced IT/OT convergence risks are expected to remain a specific concern for engineering environments. Techniques such as the "Evil PLC" attack demonstrate how programmable logic controllers can be weaponised to compromise engineering workstations, turning devices traditionally viewed as targets into vectors for deeper OT compromise (Claroty Team82, 2021). This is particularly relevant to wind farms because operational environments typically include PLCs, RTUs, HMIs, SCADA servers, protection devices, engineering tools, historian databases and remote administration pathways. Even where an attacker does not directly manipulate turbine control logic, compromise of engineering workstations or configuration tools could enable theft of project files, modification of control settings, preparation of false-command scenarios, or lateral movement into more sensitive OT segments. This reinforces the need to treat engineering workstations, vendor laptops, portable media, update channels and maintenance sessions as high-value assets rather than ordinary IT endpoints.

Cryptographic transition risk is also expected to become more visible, although it should not be overstated as an immediate operational threat within the 12–24 month outlook window. The more practical near-term concern is that offshore wind assets have long lifecycles, rely on remote access and telemetry, and may include legacy devices or vendor-managed systems that are difficult to update quickly. The EU's coordinated

roadmap for transition to post-quantum cryptography and the approval of NIST post-quantum cryptographic standards indicate that organisations operating critical and long-lived infrastructure should begin preparing inventories, transition plans and crypto-agility strategies rather than waiting for a mature quantum threat to materialise (European Commission, 2025; NIST, 2024). For offshore wind operators, the priority is therefore to understand where cryptography is used across VPNs, remote access, device authentication, firmware updates, telemetry, APIs and supplier interfaces, and to ensure that future procurement and lifecycle-management processes do not lock the sector into difficult-to-replace cryptographic dependencies.

Overall, emerging technical risks are expected to push offshore wind cybersecurity away from perimeter-oriented protection and toward continuous assurance of interconnected digital ecosystems. The key technical challenge will be maintaining trustworthy visibility and control across supplier-managed infrastructure, cloud-connected monitoring, remote engineering access, AI-assisted analysis, OT devices and long-lifecycle communication channels. For AENAON, this reinforces the value of preparedness scenarios that test compound technical failures: compromised supplier access, degraded telemetry, manipulated engineering workflows, cloud/API disruption, and loss of confidence in data used for operational decision-making.

Regulatory and Compliance Implications

Over the next 12–24 months, regulatory and compliance pressure on offshore wind cybersecurity is expected to shift from general awareness of cyber obligations toward demonstrable preparedness, auditable evidence and operationally tested response capability. This subsection will not repeat the legal framework; we defer the reader to Section 2.2 where this has been analysed. Instead, herein we summarise the main forward-looking implications for offshore wind operators, suppliers and preparedness-service providers arising from the threat outlook described in Sections 8.1–8.3.

The NIS2 Directive is expected to remain the primary driver of operator-side cybersecurity governance for offshore wind and the wider energy sector. Its practical effect is likely to be increased pressure on operators to demonstrate that cybersecurity risk management, incident handling, business continuity, supply-chain security, access control and monitoring are not only documented, but also tested and evidenced. This is particularly important for the threat scenarios identified earlier in this report, including ransomware, supplier compromise, DDoS, remote-access abuse, OT/ICS disruption and destructive activity affecting monitoring or control environments. In the context of significant incidents, NIS2 also introduces a structured reporting sequence, including an early warning within 24 hours of becoming aware of a significant incident, an incident notification within 72 hours and a final report no later than one month after submission of the incident notification (European Union, 2022).

Regulatory pressure will also increase because cybersecurity incidents may trigger overlapping notification and accountability obligations. A ransomware or data-

exfiltration incident affecting an offshore wind operator, OEM or maintenance provider may need to be assessed simultaneously as a cybersecurity incident, a personal data breach, a supply-chain event and a business-continuity disruption. Where personal data are affected, the GDPR requires controllers to notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons (European Union, 2016). This means that future preparedness will require coordinated legal, cybersecurity, operational, communications and management workflows rather than isolated technical response procedures.

The Cyber Resilience Act is expected to strengthen the product-security and supplier-assurance dimension of offshore wind cybersecurity. While many CRA obligations apply primarily to manufacturers and other economic operators placing products with digital elements on the EU market, offshore wind operators will be affected indirectly through procurement, supplier governance and lifecycle assurance expectations. Products used in wind-farm environments – including controllers, communication equipment, remote-access components, monitoring platforms, software interfaces and vendor-supplied digital services – will increasingly need to be assessed against secure-by-design, secure-by-default, vulnerability-handling, update-management, logging, access-control and software-transparency expectations. The CRA therefore reinforces the importance of supplier visibility, component transparency and vulnerability evidence across the digital supply chain (European Union, 2024a).

The AI Act is expected to become relevant where AI-enabled systems are used in cybersecurity monitoring, anomaly detection, predictive maintenance, risk assessment, operational decision-support or digital-twin environments, depending on their classification and role. The main implication for offshore wind is not that all AI-enabled tools automatically become high-risk systems, but that AI-enabled capabilities used in critical infrastructure contexts will require stronger governance around robustness, cybersecurity, human oversight, logging, transparency and post-deployment monitoring where the Act applies (European Union, 2024b). This is consistent with the emerging technical risks identified in Section 8.3, where AI-enabled systems were treated both as defensive enablers and as systems requiring assurance.

Compliance implications are therefore increasingly linked to evidence generation. Offshore wind operators and service providers will need to show not only that policies exist, but that they can identify critical assets and dependencies, understand supplier exposure, detect and classify incidents, preserve relevant logs, assess severity, coordinate internal decision-making and document response actions. This is particularly important because the threat scenarios identified in this report often affect the support layers around wind operations – such as corporate IT, remote monitoring, vendor access, satellite communications, cloud services and second-level SCADA – rather than turbine-control systems alone. Regulatory readiness will therefore depend on the ability to connect cyber

evidence to operational consequences, including loss of view, loss of remote control, degraded maintenance capability, data exposure and potential cascading effects.

In this context, AENAON's positioning as a preparedness and evidence-support environment is very timely. The project can support operators and stakeholders by enabling cyber-physical scenario analysis, supplier-risk assessment, legacy-protocol and remote-access exposure assessment, incident-response playbooks, training exercises, observability workflows and documentation practices. However, responsibility for legal compliance remains with the relevant duty bearer under each applicable instrument. This distinction is already reflected in the legal-to-operational traceability approach used in Appendix B, where AENAON actions are treated as support relationships for preparedness, validation, evidence generation, training or operational analysis, rather than as substitutes for legal compliance by operators, manufacturers, providers, deployers, controllers or processors.

Overall, the regulatory outlook reinforces the need for offshore wind cybersecurity programmes to become more evidence-driven, supplier-aware and exercise-based. The most important shift is not simply the existence of stricter legal obligations, but the practical need to demonstrate preparedness before an incident occurs and to produce reliable evidence quickly when one does. This aligns directly with AENAON's broader objective of supporting ex-ante preparedness, realistic cyber-range scenarios, risk assessment, incident response readiness and cross-stakeholder coordination for offshore wind environments.

13. Recommendations

Policy Recommendations

The report shows that offshore wind farm operators depend heavily on OEM-controlled systems, remote maintenance channels and specialised suppliers, creating concentrated cyber risks that individual operators cannot fully manage alone. Policy makers should support the development of a European framework for identifying and assessing critical ICT dependencies in offshore wind infrastructure, building on NIS2 supply chain security obligations and emerging EU discussions on high-risk suppliers. The objective should not be blanket supplier restrictions but greater transparency regarding critical functionalities, alternative sourcing options and dependency concentration risks across the sector.

Additionally, current compliance frameworks often focus on whether cybersecurity measures exist, rather than on whether specific suppliers create systemic operational dependencies. Policymakers should encourage risk assessments that consider both cybersecurity maturity and operational criticality, including the role of suppliers in remote access, SCADA support, firmware updates and restoration activities. This would help operators priritise mitigation efforts where disruptions could have the greatest impact on resilience and continuity of operations.

Finally, the findings suggest that offshore wind operators face challenges that differ from traditional IT environments, including legacy OT systems, remote access, long maintenance cycles and supplier-managed infrastructure. EU and national authorities should complement NIS2 requirements with implementation guidance and sector-specific good practices focused on operational technology, remote access governance and incident response in offshore environments. This would improve consistency of implementation while reducing unnecessary compliance burdens.

Preparedness, Exercises and Sector Coordination

Preparedness across the sector is uneven, and the survey evidence in Section 3.2 identifies one gap with particular clarity: no energy respondent had conducted a simulation or digital twin exercise, against half of the non-energy respondents. This is not a difference of degree but an absence, and it sits directly in the path of what a federated digital twin cyber range is designed to provide.

Two consequences follow. First, sector exercise programmes should move beyond the tabletop formats that currently dominate, towards simulation-based rehearsal in which remote access compromise and supplier disruption can be played through without operational risk. Second, awareness is a precondition for adoption: energy respondents cite the lack of testing environments as a gap notably less often than others do, which suggests the absence is not yet widely recognised as a vulnerability. Making that gap visible is itself part of the intervention.



Exercise scenarios should be built around the exposure the sector actually reports — OEM and third-party remote access, supplier compromise, and legacy OT systems operating on extended patch cycles — rather than around generic enterprise incident scripts. Because the dependency that defines the exposure is shared across operators and their OEM partners, coordination should extend beyond individual organisations to shared scenario libraries, common exercise formats and joint exercises spanning the operator–vendor boundary.

Scenario development should incorporate AI-enabled attack patterns now, ahead of the sector adopting AI in operations, rather than in response to it. The evidence in Section 4.8 indicates a time-limited window: frontier models already execute multi-stage intrusions against weakly defended environments but have not yet demonstrated the same capability against operational technology. Detection playbooks, incident response procedures and analyst familiarity take time to build, and building them during that window is materially cheaper than building them under pressure afterwards. Exercises should include compressed-patch-window scenarios, in which a vulnerability is exploited before remediation is operationally feasible, and supplier-side AI scenarios, in which the initial access originates from a partner's own systems.

Operator and Supplier Measures

Policy and exercise measures address the sector level, but the exposures the evidence identifies most consistently sit within the control of individual operators and their suppliers. Across the incident record, the survey responses and the attack-surface analysis in Section 6, four exposures recur: OEM and third-party remote access, concentrated supplier dependency, legacy OT operating on extended patch cycles, and limited visibility of assets and dependencies. The measures below follow from that evidence base rather than from generic good practice, and are intended to complement rather than duplicate NIS2 Article 21 obligations.

Remote access into operational environments should be brokered, individually attributable, multi-factor authenticated and time-bounded to the maintenance window it serves, with standing supplier access replaced by access granted on request and revoked on completion. Operators should maintain a current inventory of OT assets, firmware versions and the external parties able to reach them, since limited asset visibility is both the most frequently cited gap in the survey and a precondition for every other measure here. Supplier assurance should extend beyond questionnaire-based maturity checks to the operational criticality of each supplier, covering remote-access rights, firmware and update provenance, and the supplier's own incident notification commitments. Network segmentation should isolate turbine control, SCADA and remote-monitoring environments from corporate IT and from one another, so that an intrusion originating in enterprise systems or at a single supplier cannot propagate across the asset base. Recovery arrangements should be tested rather than documented, with offline and integrity-verified backups of controller configurations and firmware, and restoration times validated against the constraint that physical access offshore depends on vessel availability and weather

References

AENAON Consortium. Description of Action (Annex 1 to the Grant Agreement), Grant Agreement No. 101249723.

AENAON D4.1, Open Call Methodology Report, sections on realistic operational validation, sector-specific cybersecurity scenarios, Open Call testing and coordinated resilience activities. Internal project source.

AI Security Institute. (2026). Our evaluation of Claude Mythos Preview's cyber capabilities. UK AI Security Institute. https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

BMWE. (2026). The Hamburg Declaration – North Sea Summit 2026. German Federal Ministry for Economic Affairs and Energy. https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Downloads/M-O/nordsee-gipfel-2026/the-hamburg-declaration.pdf

Borch, K., Munk, A.K. & Dahlgaard, V. (2020). Mapping wind-power controversies on social media: Facebook as a powerful mobilizer of local resistance. Energy Policy, 138, 111223. https://doi.org/10.1016/j.enpol.2019.111223

CERT Polska. (2026). Energy Sector Incident Report – 29 December 2025. CERT Polska / NASK. https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

CISA, NSA, FBI and international partners. (2024). PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Cybersecurity Advisory AA24-038A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

CISA, FBI. (2023). #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability. Cybersecurity Advisory AA23-158A. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

CISA. (2021). Kaseya VSA Supply-Chain Ransomware Attack. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/alerts/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack

CISA. (2022) Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector. Alert AA22-083A, Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a

Cisco Talos. (2020). PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors. Cisco Talos Intelligence Group. https://blog.talosintelligence.com/poetrat-covid-19-lures/

Claroty Team82. (2021). Evil PLC Attack: Weaponizing PLCs. https://claroty.com/team82/research/white-papers/evil-plc-attack-weaponizing-plcs

Cloud Security Alliance, SANS Institute, [un]prompted and OWASP GenAI Security Project. (2026). Emergency Strategy Briefing as AI-Driven Vulnerability Discovery Compresses Exploit Timelines from Weeks to Hours. https://cloudsecurityalliance.org/press-releases/2026/04/14/sans-institute-cloud-security-alliance-un-prompted-and-owasp-genai-security-project-release-emergency-strategy-briefing-as-ai-driven-vulnerability-discovery-compresses-exploit-timelines-from-weeks-to-hours

Cloud Security Alliance, SANS Institute, [un]prompted and OWASP GenAI Security Project. (2026). The AI Vulnerability Storm: Building a Mythos-Ready Security Program. CC BY-NC 4.0.

Council of the European Union. (2023). Maritime security: Council approves revised EU strategy and action plan. **https://www.consilium.europa.eu/en/press/press-releases/2023/10/24/maritime-security-council-approves-revised-eu-strategy-and-action-plan/**

Cybersecurity Dive. (2024). Halliburton incurs about $35M in expenses related to August cyberattack. Cybersecurity Dive. **https://www.cybersecuritydive.com/news/halliburton-35-million-cyberattack/732397/**

Datta, P. & Acton, T. (2026). Hades casts its long shadow: The global ransomware nexus. Journal of Information Technology Teaching Cases. https://doi.org/10.1177/20438869261436824

de Lemos, V. & Ignaczak, L. (2023). An analysis of the public consequences of cybersecurity incidents in Brazil. Social Network Analysis and Mining, 13, 106. https://doi.org/10.1007/s13278-023-01113-9

Deutsche Windtechnik. (2022). Cyber attack on Deutsche Windtechnik [press release]. https://www.deutsche-windtechnik.com/en/news/press-releases/details/cyber-attack-on-deutsche-windtechnik/

E3C. (2020). GB Power System Disruption – 9 August 2019: Final Report. UK Energy Emergencies Executive Committee. **https://www.gov.uk/government/publications/great-britain-power-system-disruption-9-august-2019**

Ebrahimi, S. & Eshghi, K. (2022). A meta-analysis of the factors influencing the impact of security breach announcements on stock returns of firms. Electronic Markets, 32(4), 2357-2380. https://doi.org/10.1007/s12525-022-00550-2

Electrica Group. (2024). Ransomware attack [threat intelligence report CB25-01]. CERT-EU. https://cert.europa.eu/publications/threat-intelligence/cb25-01/

Energy Institute. (2026). UK secures 8.4 GW of offshore wind at strike prices as low as £89.49/MWh. New Energy World. https://knowledge.energyinst.org/new-energy-world/article?id=140068

ENISA. (2024). ENISA Threat Landscape 2024, 12th edition, 19 September 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

ENISA. Multilayer Framework for Good Cybersecurity Practices for AI, June 2023. ISBN 978-92-9204-619-4.

European Commission. (2019). The European Green Deal. COM(2019) 640 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:640:FIN

European Commission. (2020). An EU Strategy to harness the potential of offshore renewable energy for a climate neutral future. COM(2020) 741 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0741

European Commission. (2022). REPowerEU Plan. COM(2022) 230 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0230

European Commission. (2023). European Wind Power Action Plan. COM(2023) 669 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023DC0669

European Commission. (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

European Commission. (2026). Proposal for a Regulation of the European Parliament and of the Council on the European Cybersecurity Act. COM(2026) 11 final. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Union. (2023). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

European Union. (2024a). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

European Union. (2024b). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Freeman, S. G., Kress-Weitenhagen, M. A., Gentle, J. P., Culler, M. J., Egan, M. M. and Stolworthy, R. V. (2024). Attack Surface of Wind Energy Technologies in the United States. Idaho National Laboratory, INL/RPT-24-76133-Revision-0. https://www.osti.gov/biblio/2297403

Geri, M. (2024). Understanding Russian hybrid warfare against Europe in the energy sector and in the future energy–resources–climate nexus. Journal of Strategic Security, 17(3), 15–34. https://doi.org/10.5038/1944-0472.17.3.2270

Goel, S. & Shawky, H.A. (2009). Estimating the market impact of security breach announcements on firm values. Information & Management, 46(7), 404-410. https://doi.org/10.1016/j.im.2009.06.005

Goodell, J.W. & Corbet, S. (2022). Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. Finance Research Letters, 51, 103329. https://doi.org/10.1016/j.frl.2022.103329

Gundur, R. et al. (2026). The Commercialization of Ransomware: From Spray-and-Prey to Big Game Hunting to the Ransom Bazaar. Crime & Delinquency.

Hitachi Energy. (2023). Third-party cybersecurity incident. https://www.hitachienergy.com/news-and-events/features/2023/03/third-party-cybersecurity-incident

Humpal, J. (2026, March 25). From Earth Liberation to Accelerationism: A High-Level Review of Fifty Years of Domestic Infrastructure Terrorism. CTC Sentinel, 19(3). Combating Terrorism Center at West Point. **https://ctc.westpoint.edu/from-earth-liberation-to-accelerationism-a-high-level-review-of-fifty-years-of-domestic-infrastructure-terrorism/**

Ivanov, G. and Poita, Y. (2025). Ensuring the Security of Onshore and Offshore Wind Farms in the Context of War or Terrorism. Sustainable Marine Structures, 7(2), pp. 45–62. https://doi.org/10.36956/sms.v7i2.1865

Janvrin, D.J. et al. (2026). Colonial Pipeline: Responding to a Ransomware Attack in the Energy Sector. Issues in Accounting Education, 41(2), 131-145. **https://doi.org/10.2308/ISSUES-2025-014**

Lakshmanan, R. (2021). Hackers Breached Colonial Pipeline Using Compromised VPN Password. The Hacker News. https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

Knack, A., Syn, Y. K. H. and Tam, K. (2024). Enhancing the Cyber Resilience of Offshore Wind. CETaS Research Reports, The Alan Turing Institute. https://cetas.turing.ac.uk/sites/default/files/2024-06/cetas_research_report_-_enhancing_the_cyber_resilience_of_offshore_wind.pdf

Kulev, N., and Sill Torres, F. Investigation of high-impact low-probability disturbances in offshore wind farms. MARESEC 2022 / Zenodo, 2022. DOI: 10.5281/zenodo.7149239. https://zenodo.org/record/7149239

Kulev, N., Reuter, A., Eichhorn, O., Engler, E., and Wrede, C. P. (2020). Non-resilient behavior of offshore wind farms due to cyber-physical attacks. 8th REA Symposium on Resilience Engineering. DOI: 10.15626/rea8.22. https://elib.dlr.de/129879/

Marsili, M. (2025). Cognitive Warfare, Disinformation, and Corporate Influence in Europe's Energy Transition: Information Control, Regulation, and Human Rights Implications. Applied Cybersecurity & Internet Governance, 4(1). https://doi.org/10.60097/ACIG/214045

Martinez, A. & Iglesias, G. (2022). Mapping of the levelised cost of energy for floating offshore wind in the European Atlantic. Renewable and Sustainable Energy Reviews. https://www.sciencedirect.com/science/article/abs/pii/S1364032121011564

Masuch, K. et al. (2022). Apologize or justify? Examining the impact of data breach response actions on stock value of affected companies. Computers & Security, 112, 102502. https://doi.org/10.1016/j.cose.2021.102502

Meland, P.H., Bayoumy, Y.F.F. & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. Computers & Security, 92, 101762. https://doi.org/10.1016/j.cose.2020.101762

Meurs, T. et al. (2024). Deception in double extortion ransomware attacks: An analysis of profitability and credibility. Computers & Security, 138, 103670. https://doi.org/10.1016/j.cose.2023.103670

Miętkiewicz, R. (2025). Hybrid threats in the Baltic Sea. The results of analysis of countermeasure options. Terroryzm.

Muktadir-Al-Mukit, D. & Ali, M.H. (2025). The Dynamics of Stock Market Responses Following the Cyber-Attacks News: Evidence from Event Study. Information Systems Frontiers. https://doi.org/10.1007/s10796-025-10639-6

Muncaster, P. (2026, 26 January). Wiper attack on Polish power grid linked to Russia's Sandworm. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/wiper-attack-polish-power-grid/

National Grid ESO. (2019). Technical Report on the events of 9 August 2019. National Grid Electricity System Operator. https://www.nationalgrideso.com/document/152346/download

NATO. (2025). NATO launches "Baltic Sentry" to increase critical infrastructure security. https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security

NCSC. (2022). Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion. UK National Cyber Security Centre. https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion

NIST. (2024). Post-Quantum Cryptography FIPS Approved. National Institute of Standards and Technology. https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

NIST. SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security. National Institute of Standards and Technology, 2023. https://www.nist.gov/publications/guide-operational-technology-ot-security

Nordex SE. (2022). Update on cyber security incident [company statement]. https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/

Ofgem. (2020). Investigation into 9 August 2019 power outage – final report. Office of Gas and Electricity Markets. https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage

Oosthoek, K. et al. (2022). A Tale of Two Markets: Investigating the Ransomware Payments Economy. Communications of the ACM.

OpenAI. (2026). Hugging Face model evaluation security incident. https://openai.com/index/hugging-face-model-evaluation-security-incident/

Raggi, M. and Scenarelli, S. (2022). Rising Tide: Chasing the Currents of Espionage in the South China Sea. Proofpoint. https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea

Reuters / Euronews. Satellite outage knocks out thousands of Enercon's wind turbines. Euronews, 28 February 2022. https://www.euronews.com/next/2022/02/28/ukraine-crisis-cyber-enercon

Sabev, E., Trifonov, R., Pavlova, G. and Rainova, K. (2021). Cybersecurity Analysis of Wind Farm SCADA Systems. 2021 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, pp. 1–5. IEEE. https://doi.org/10.1109/InfoTech52438.2021.9548589

Sanghvi, A., Naughton, B., Glenn, C., Gentle, J., Johnson, J., Stoddard, J., White, J., Hilbert, N., Freeman, S., Hansen, S. and Sheng, S. (2020). Roadmap for Wind Cybersecurity. U.S. Department of Energy. https://doi.org/10.2172/1647705

Shafiee, M. et al. (2025). Cyber Resilience of Wind Energy Infrastructure: Challenges and Mitigation Strategies. https://doi.org/10.1109/ICAC65379.2025.11196193

Slovenske Elektrarne / HSE. (2023). Ransomware attack [incident coverage]. https://www.helpnetsecurity.com/2023/11/28/slovenian-power-company-ransomware/

Staggs, J. et al. (2017). Wind farm security: attack surface, targets, scenarios and mitigation. https://doi.org/10.1016/j.ijcip.2017.03.001

U.S. Department of Energy. (2020). Wind Energy Cybersecurity Roadmap. https://www.energy.gov/documents/wind-energy-cybersecurity-roadmap-2020v3pdf

Venkatachary, S.K. et al. (2017). Economic Impacts of Cyber Security in Energy Sector: A Review. International Journal of Energy Economics and Policy, 7(5), 250-262. https://www.econjournals.com/index.php/ijeep/article/view/5283

Venkatachary, S.K. et al. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures — Cybersecurity frameworks and economics — Comprehensive review. International Journal of Critical Infrastructure Protection, 45, 100677. https://doi.org/10.1016/j.ijcip.2024.100677

Vestas. (2021). Update on cyber security incident [company statement]. https://www.vestas.com/en/media/company-news/2021/update-on-cyber-security-incident-c3457795

Viasat. KA-SAT Network cyber-attack overview. Viasat, 30 March 2022. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/

WindEurope. (2025a). Delivering a cost-effective energy system for Europe. https://windeurope.org/data/products/energy-system-costs/

WindEurope. (2025b). Poland powers ahead: first offshore wind auction delivers strong results. **https://windeurope.org/news/poland-powers-ahead-first-offshore-wind-auction-delivers-strong-results/**

WindEurope. (2026). Wind energy in Europe: 2025 Statistics and the outlook for 2026-2030. WindEurope, February 2026. https://windeurope.org/data/products/wind-energy-in-europe-2025-statistics-and-the-outlook-for-2026-2030/

Winter, K. et al. (2024). Public agreement with misinformation about wind farms. Nature Communications, 15, 8888. https://doi.org/10.1038/s41467-024-53278-2

Yurrebaso, X., Ibañez, F. & Longueira-Romero, Á. (2025). Substation Bill of Materials: A novel approach to managing supply chain cyber-risks on IEC 61850 digital substations. arXiv:2503.19638. **https://arxiv.org/abs/2503.19638**

Zero Day Clock. (2026). From vulnerability to exploitation: time-to-exploit trends across confirmed-exploited CVEs. **https://zerodayclock.com**

Appendix A – Detailed Methodology

This annex explains the methodology used to develop the report. The approach followed the logic of the ENISA Cybersecurity Threat Landscape (CTL) methodology, particularly its structured process for defining intelligence needs, collecting information, processing and categorising evidence, analysing findings, and documenting limitations.

The methodology brought together three main sources of evidence: desk research on cyber incidents relevant to offshore wind farms and the wider wind energy ecosystem, passive open-source intelligence research on exposed equipment and services relevant to the sector, and input from industry stakeholders through questionnaires, project partners, and sector events.

The aim was to build a sector-specific view of the cyber threats affecting offshore wind. This meant looking not only at incidents that have been publicly reported, but also at less visible issues such as attempted attacks, near misses, supplier-related disruptions, unreported incidents, and events that may not have fully materialised but still provide useful insight into the threat environment.

Intelligence Direction

The intelligence direction phase set the scope, objectives, and key questions for the research. In line with the ENISA CTL methodology, this phase clarified what information was needed, why it mattered, and how it would support the final assessment.

The main objective was to understand the cyber threat landscape affecting offshore wind farms from both an evidence-based and industry-informed perspective. The research therefore examined incidents affecting offshore wind farms, wind energy operators, offshore energy infrastructure, maritime systems, ports, suppliers, and related digital services. It also considered which systems and services used in the offshore wind ecosystem may remain exposed online, which threats are viewed by industry as most relevant, and which assets stakeholders consider most important to protect.

The scope covered offshore wind farms, operational technology environments, remote monitoring and control systems, maritime and port interfaces, energy-sector suppliers, maintenance providers, and the digital services that support offshore wind operations.

A key part of the methodology was to consider both direct and indirect cyber threats. This was necessary because an incident affecting offshore wind does not always have to target the wind farm itself. A disruption can originate from a supplier, a communications link, a remote access service, a maintenance platform, a vessel, a port, a substation, or a corporate IT system that supports operational continuity. For this reason, the assessment looked beyond the wind farm boundary and considered the wider ecosystem on which offshore wind operations depend.

Collection Phase

The collection phase combined publicly available sources, passive open-source intelligence, and direct stakeholder input.

Desk research was used to identify publicly reported cyber incidents relevant to offshore wind and adjacent sectors. The sources reviewed included public reports, cybersecurity advisories, threat intelligence publications, media reporting, sector analyses, and information released by public authorities or affected organisations where available.

This research focused on incidents involving offshore wind operators, asset owners, wind energy companies, suppliers, maritime and port infrastructure, energy-sector operational technology, industrial control systems, remote monitoring platforms, and maintenance services. Attention was given to ransomware, data theft, supply chain compromise, disruption events, exposed services, and attacks affecting remote access or industrial environments.

The desk research provided a baseline for understanding documented cyber activity affecting the sector. However, public reporting was treated carefully. Many incidents are not disclosed, are disclosed only in limited terms, or are reported without enough technical detail to understand exactly what happened. In some cases, it is also difficult to determine whether an incident affected offshore wind operations directly or only a related corporate, supplier, or infrastructure environment.

A passive open-source intelligence review was also carried out using Shodan. This was used to identify examples of internet-exposed equipment, interfaces, and services associated with technologies relevant to offshore wind and industrial operations.

This activity was strictly passive. No attempt was made to access systems, bypass authentication, interact with devices, conduct vulnerability testing, perform active scanning, or validate whether any system was exploitable. The purpose was not to assess or attribute weaknesses to individual organisations. Instead, the review supported sector-level observations about exposure risk, asset visibility, remote access practices, legacy equipment, and the need for stronger control over externally reachable systems.

Stakeholder input was collected through questionnaires distributed via project partners and relevant events. These questionnaires were aimed at organisations and professionals involved in offshore wind operations, cybersecurity, engineering, maintenance, supply chain services, and related activities.

The questionnaire process was designed to capture how stakeholders perceive the likelihood and impact of different cyber threats, which threat scenarios they consider most important, and which assets and systems they see as most critical to protect. It also sought information about cyber incidents, attempted attacks, near misses, suspicious activity, gaps in protection, detection and response, and expectations for improved information sharing across the sector.

This input was important because the public record alone does not provide a complete picture of cyber activity in offshore wind. Some incidents remain internal, some are handled by suppliers, and others never reach the threshold for public disclosure. In other cases, events may be classified as operational or technical disruptions rather than cybersecurity incidents, even when cyber risk is relevant.

Processing & Taxonomy

The processing phase involved reviewing, filtering, structuring, and categorising the information collected from all sources. The objective was to turn raw information into a consistent evidence base that could support analysis.

Information gathered through desk research was reviewed for relevance to offshore wind, offshore energy, maritime operations, industrial control systems, remote access, and supply chain exposure. Incidents that were too generic, insufficiently substantiated, or unrelated to the sector were excluded or treated only as background context.

The collected information was organised according to several analytical dimensions. These included the type of threat, such as ransomware, phishing, supply chain compromise, unauthorised access, data theft, denial of service, malware, and exploitation of exposed services. The analysis also considered the affected environment, including corporate IT, operational technology, industrial control systems, remote monitoring platforms, maritime systems, cloud services, and supplier infrastructure.

Potential impacts were also categorised. These included loss of availability, safety implications, financial loss, reputational damage, data compromise, disruption to maintenance, and reduced operational visibility. Attack vectors were assessed as well, including remote access abuse, exposed services, credential compromise, third-party compromise, malicious attachments, exploitation of vulnerabilities, and misconfiguration.

Stakeholder feedback was processed to identify recurring themes, shared concerns, and differences between stakeholder groups where relevant. Focus was given to how respondents ranked possible threats and which assets they identified as most important to protect. This made it possible to compare publicly observed incidents with industry perception and operational priorities.

The Shodan-based research was processed at category level rather than organisation level. The analysis focused on types of exposed technologies and services, not on identifying or naming specific owners. This reduced the risk of disclosing sensitive information while still allowing the report to identify relevant exposure patterns.

Analytical techniques

The analysis combined qualitative assessment, cross-source comparison, and sector-specific interpretation.

The first step was to compare publicly reported incidents with the operational reality of offshore wind. This helped distinguish incidents that were directly relevant to offshore wind

from those that were indirectly relevant through dependencies such as ports, vessels, suppliers, remote operations, or wider energy-sector infrastructure.

The second step was to compare incident findings with the passive open-source review. This helped assess whether known attack vectors, including exposed remote access services and vulnerable internet-facing systems, remain plausible concerns for the sector.

The third step was to analyse questionnaire responses and stakeholder feedback. This provided insight into how industry stakeholders perceive cyber threats, which scenarios they consider most concerning, and which assets they believe should be prioritised for protection.

The analysis considered the difference between threats that are frequently observed or publicly reported, threats that stakeholders perceive as highly likely, and threats that may occur less often but could have severe operational, safety, or financial consequences. It also considered which assets are technically critical to offshore wind operations and which assets are viewed by industry as needing priority protection.

The methodology also accounted for the gap between reported incidents and unreported or partially materialised events. This was important because cyber risk in offshore wind cannot be assessed only through public incident databases. Near misses, attempted intrusions, supplier disruptions, and suspicious activity may provide important indicators of the real threat environment, even when they do not lead to public disclosure.

Overall, the analysis looked for incident patterns, recurring exposure themes, common stakeholder concerns, and protection priorities across IT, OT, remote access, communications, maintenance, and supply chain systems. The final assessment was based on triangulation across the three main evidence streams: public incident information, passive exposure research, and direct industry feedback. This helped reduce reliance on any single source and supported a more balanced understanding of the offshore wind cyber threat landscape.

The questionnaire responses were additionally subject to a formal statistical treatment. In summary, responses were tested for whether observed patterns differ from what chance would produce; the ranked questions were summarised using composite scoring and assessed for the degree of agreement between respondents; hierarchical clustering was used to identify tiers of concern rather than precise orderings; and groups were compared pairwise, with correction applied for multiple testing and effect sizes reported throughout. Given the sample size, the treatment is powered to detect only medium-to-large differences, and directionally consistent results that fall short of significance are reported as such. All findings are accordingly presented as exploratory and hypothesis-generating rather than confirmatory.

Limitations

The methodology has several limitations that should be considered when interpreting the findings. They fall into three groups: constraints specific to each of the three evidence

streams, constraints arising from the statistical treatment of the questionnaire responses, and constraints inherent to the sector itself.

The desk research is bounded by what has been made public. Reported cyber incidents do not represent the full threat landscape. Many incidents are not disclosed, are disclosed only after a significant delay, or are reported without enough technical detail to support a full assessment. In some cases, it may not be possible to determine whether an incident affected offshore wind operations directly or only a related corporate, supplier, or infrastructure environment.

The OSINT scanning is subject to two further constraints. It reflects a single collection window, as noted in Section 1.5, so it describes exposure at a point in time rather than continuously; and the presence of equipment or services in the scan results indicates potential exposure only. It does not prove that a system is vulnerable, actively used in offshore wind operations, misconfigured, or insufficiently protected. No validation or testing was performed, and no conclusions were drawn about the security posture of specific organisations.

Questionnaire results depend on the number, profile, and experience of respondents. The findings reflect the views of participating stakeholders and may not fully represent the entire offshore wind sector. Responses may also be influenced by the respondent's role, organisational maturity, previous incident experience, or level of cybersecurity awareness. Participation was voluntary, so organisations with higher security awareness or greater concern about cyber threats may be over-represented, which would tend to raise perceived threat severity across the board.

Four constraints apply specifically to the statistical treatment of the questionnaire and should be borne in mind wherever its results are cited in this report. First, the sample supports the detection of only medium-to-large differences. Several findings that point consistently in one direction, including the energy group's heavier weighting of remote access compromise, fall short of conventional significance thresholds because of sample size rather than because no effect exists; a substantially larger sample would be needed before any result here could be treated as confirmatory.

Second, the comparison groups are uneven. The sector-adjacent group is both small and internally diverse, and results involving it are descriptive rather than inferential. The three-group analysis was run in part to confirm that the broader energy and non-energy differences are not an artefact of the defence respondents' distinct profile, and it does confirm this, but comparisons resting on the smallest group should not be relied upon.

Third, the ranking questions asked respondents to choose a top three, so items left unranked cannot be assumed to be regarded as least severe. The analysis assigns those items a shared mid-range position, which has the side effect of grouping rarely selected items together irrespective of whether respondents view them as comparable. The lower tiers of the threat and entry point orderings should therefore be read as "seldom prioritised" rather than as a genuine ranking.

Fourth, no causal claims can be drawn. The association between third-party access exposure and the salience of remote access as a threat is substantively persuasive and consistent across the analysis, but a cross-sectional survey cannot distinguish between exposure driving perception, perception driving disclosure of exposure, and both being driven by sector affiliation.

Four constraints apply to the statistical treatment of those responses, and should be borne in mind wherever its results are cited elsewhere in this report.

First, the sample supports the detection of only medium-to-large differences. Findings that point consistently in one direction but fall short of conventional significance — the energy group's heavier weighting of remote access compromise among them — reflect the size of the sample rather than the absence of an effect. No result reported here should be treated as confirmatory.

Second, the comparison groups are uneven. The sector-adjacent group is small and internally diverse, so results involving it are descriptive rather than inferential. Separating the defence respondents from the wider non-energy group served in part as a check that the energy findings are not an artefact of the defence profile; that check passes, but comparisons resting on the smallest group should not be relied upon.

Third, respondents were asked for a top three, so items left unranked cannot be read as those regarded least severe. The analysis assigns unranked items a shared mid-range position, which groups rarely-selected items together whether or not respondents see them as comparable. The lower tiers of the threat and entry point orderings should therefore be read as seldom prioritised rather than as a ranking.

Fourth, no causal claims can be drawn. The association between third-party access exposure and the salience of remote access as a threat is persuasive and consistent across the analysis, but a cross-sectional survey cannot separate exposure driving perception from perception driving disclosure of exposure, or from both being driven by sector affiliation.

There are also classification challenges. Incidents that do not fully materialise, near misses, and suspected cyber events can be difficult to classify consistently. Stakeholders may interpret similar events differently, especially where the boundary between technical failure, operational disruption, and cybersecurity incident is unclear.

Another limitation is the highly interconnected nature of offshore wind. Cyber risks may originate outside the direct control of asset owners, including through suppliers, contractors, remote service providers, ports, vessels, communications providers, and cloud platforms. This makes attribution, impact assessment, and prioritisation more complex.

Despite these limitations, the combination of desk research, passive open-source intelligence, and stakeholder engagement provides a stronger basis for analysis than public

reporting alone. The methodology supports a sector-level view of cyber threats, exposure patterns, stakeholder concerns, and protection priorities relevant to offshore wind farms.

Appendix B – Baseline legal obligations under NIS2 and CRA

This annex sets out the baseline legal obligations under the NIS2 Directive and the Cyber Resilience Act that apply to every threat category identified in this deliverable's threat landscape (Section 4), because these obligations attach to the operation of the wind farm and its digital products generally, rather than to any single threat (European Union, 2022; European Union, 2024a). Each obligation is linked to the AENAON capability area that supports it and classified as Direct or Partial, reflecting the extent to which AENAON's planned capabilities support, validate or evidence the underlying legal duty. This mapping is intended to support transparency and reviewability; it does not create additional legal obligations for the consortium, operators, manufacturers, providers or public authorities, and legal responsibility remains with the relevant duty bearer under the applicable instrument. Table 4 defines the coverage categories used in this annex, Table 5 the capability areas applied in the mapping, and Table 6 presents the resulting obligation-level mapping.

Table 4: Coverage categories

Coverage category	Meaning
Direct	The requirement is operationally central to the threat category and is directly supported, validated or monitored through an AENAON capability.
Partial	AENAON contributes through assessment, validation, observability, preparedness support or evidence generation, but implementation responsibility remains partly or mainly with another actor under the relevant legal instrument.
Out of Scope	The requirement is relevant for regulatory completeness but cannot be implemented by AENAON - for example, a manufacturer-side, competent-authority or public-authority obligation.

Table 5: Capability areas used in the mapping

Capability area	Role in the mapping
DTV – Digital Twins & Virtualisation Services (T3.1)	Supports requirements involving cyber-physical scenario modelling, representation of grid and operational interdependencies, continuity/restoration rehearsal and resilience validation in a virtualised environment.

Capability area	Role in the mapping
VDPT – Vulnerability Discovery & Penetration Testing Services (T3.2)	Supports requirements involving vulnerability identification and handling, security testing, attack-surface reduction, secure-configuration validation, component transparency (SBOM/CBOM) and update-mechanism assessment.
SACR – Security Awareness & Cyber Range Services (T3.3)	Supports governance, cyber-hygiene and training-related requirements, including management-body training. The Interactive Cyber Range Training Programme (ICRTP, T2.4) is delivered through this service area.
TRA – Threat & Risk Assessment Services (T3.4)	Supports requirements involving risk analysis, proportionality, supplier and third-party risk, cascading-risk assessment, cryptographic-posture and legacy-protocol assessment, and effectiveness evaluation.
RMCM – Risk/Threat Monitoring & Cyberattack Management Services (T3.5)	Supports requirements involving incident detection, handling, investigation and evidence generation, logging and observability, notification/reporting workflows and advisory ingestion.
Project-level actions	Documentation and governance measures taken at consortium level that are not delivered through a preparedness service.

Table 6: Baseline legal obligations under NIS2 and CRA

Legal source	Provision	Requirement summary	Capability area	Coverage
NIS2	Art. 20(1)	Management-body approval and oversight of cybersecurity risk-management measures; liability for infringements.	TRA, SACR	Partial
NIS2	Art. 20(2)	Mandatory cybersecurity training for members of the management body.	SACR	Direct
NIS2	Art. 21(1)	Appropriate and proportionate technical, operational and organisational cybersecurity risk-management measures.	TRA	Direct
NIS2	Art. 21(1), 2nd subpara.	Security level appropriate to the risk, taking into account state of the art and cost.	TRA	Partial
NIS2	Art. 21(2)(a)	Policies on risk analysis and information-system security (all-hazards approach).	TRA	Direct

Legal source	Provision	Requirement summary	Capability area	Coverage
NIS2	Art. 21(2)(a) — OWF interpretation	Risk analysis to cover cyber-physical and grid-level interdependencies with the bulk electricity system.	TRA, DTV	Direct
NIS2	Art. 21(2)(b)	Incident handling.	RMCM	Direct
NIS2	Art. 21(2)(c)	Business continuity, backup management, disaster recovery and crisis management.	TRA, DTV	Partial
NIS2	Art. 21(2)(d)	Supply-chain security covering relationships with direct suppliers and service providers.	TRA	Direct
NIS2	Art. 21(2)(e)	Security in acquisition, development and maintenance, including vulnerability handling and disclosure.	VDPT, TRA	Direct
NIS2	Art. 21(2)(f)	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	VDPT, TRA	Direct
NIS2	Art. 21(2)(g)	Basic cyber-hygiene practices and cybersecurity training.	SACR	Direct
NIS2	Art. 21(2)(g) — OWF/TCA interpretation	Cyber hygiene to include transient cyber asset (TCA) management for the offshore environment.	TRA, VDPT	Direct
NIS2	Art. 21(2)(h)	Policies and procedures on the use of cryptography and, where appropriate, encryption.	TRA	Partial
NIS2	Art. 21(2)(h) — OWF interpretation	Cryptography policy to address legacy cleartext or weakly-authenticated industrial protocols (replacement or compensating control).	TRA, VDPT	Direct
NIS2	Art. 21(2)(i)	Human-resources security, access-control policies and asset management.	RMCM	Direct
NIS2	Art. 21(2)(j)	Multi-factor or continuous authentication and secured communications, where appropriate.	RMCM	Partial
NIS2	Art. 21(3)	Account for supplier-specific vulnerabilities and the overall quality of suppliers' cybersecurity practices.	TRA	Direct



Legal source	Provision	Requirement summary	Capability area	Coverage
NIS2	Art. 23(1)	Notify the CSIRT or competent authority of any significant incident without undue delay.	RMCM	Direct
NIS2	Art. 23(2)	Communicate to affected service recipients measures or remedies against a significant cyber threat, where applicable.	RMCM	Partial
NIS2	Art. 23(3)	Significance criteria for incidents (severe operational disruption, financial loss, or damage to others).	RMCM	Direct
NIS2	Art. 23(4)(a)	24-hour early warning indicating a suspected malicious cause or possible cross-border impact.	RMCM	Direct
NIS2	Art. 23(4)(b)	72-hour incident notification with an initial assessment of severity, impact and indicators of compromise.	RMCM	Direct
NIS2	Art. 23(4)(c)	Intermediate report on status updates upon request of the CSIRT or competent authority.	RMCM	Direct
NIS2	Art. 23(4)(d)	Final report within one month: detailed description, severity, root cause, mitigations and cross-border impact.	RMCM	Direct
NIS2	Art. 23(4)(e)	Progress report for ongoing incidents and a final report within one month of handling.	RMCM	Direct
CRA	Annex I, Part I, point (1)	Risk-based secure design, development and production of products with digital elements.	TRA	Partial
CRA	Annex I, Part I, point (2)(a)	Place products on the market without known exploitable vulnerabilities.	VDPT	Direct
CRA	Annex I, Part I, point (2)(b)	Secure-by-default configuration, including the possibility to reset to the original state.	VDPT	Direct
CRA	Annex I, Part I, point (2)(c)	Address vulnerabilities through security updates, including automatic updates where applicable.	RMCM	Partial



Legal source	Provision	Requirement summary	Capability area	Coverage
CRA	Annex I, Part I, point (2)(d)	Protection from unauthorised access via authentication or identity-and-access management; report unauthorised access.	RMCM	Direct
CRA	Annex I, Part I, point (2)(e)	Protect confidentiality of stored, transmitted or processed data, including by encryption.	TRA	Partial
CRA	Annex I, Part I, point (2)(f)	Protect integrity of data, commands, programs and configuration; report corruptions.	RMCM	Direct
CRA	Annex I, Part I, point (2)(g)	Process only data that are adequate, relevant and limited to the purpose (data minimisation).	Project-level actions	Partial
CRA	Annex I, Part I, point (2)(h)	Protect availability of essential functions, including resilience against denial-of-service.	DTV, VDPT	Direct
CRA	Annex I, Part I, point (2)(i)	Minimise the product's negative impact on the availability of other devices or networks.	TRA	Partial
CRA	Annex I, Part I, point (2)(j)	Limit attack surfaces, including external interfaces.	VDPT	Direct
CRA	Annex I, Part I, point (2)(k)	Reduce incident impact using appropriate exploitation-mitigation mechanisms.	TRA, RMCM	Partial
CRA	Annex I, Part I, point (2)(l)	Record and monitor relevant internal security activity (logging) with a user opt-out.	RMCM	Direct
CRA	Annex I, Part I, point (2)(m)	Enable users to securely and permanently delete data and settings.	Out-of-scope classification	Out of scope
CRA	Annex I, Part II, point (1)	Identify and document vulnerabilities and components, including a software bill of materials (SBOM).	VDPT, RMCM	Direct
CRA	Annex I, Part II, point (2)	Address and remediate vulnerabilities without delay through security updates.	VDPT, RMCM	Partial
CRA	Annex I, Part II, point (3)	Apply effective and regular security testing and review of the product.	VDPT	Partial



Legal source	Provision	Requirement summary	Capability area	Coverage
CRA	Annex I, Part II, point (4)	Publicly disclose information about fixed vulnerabilities once an update is available.	RMCM	Partial
CRA	Annex I, Part II, point (5)	Establish and enforce a coordinated vulnerability disclosure policy.	Out-of-scope classification	Out of scope
CRA	Annex I, Part II, point (6)	Facilitate sharing of vulnerability information, including a reporting contact address.	Out-of-scope classification	Out of scope
CRA	Annex I, Part II, point (7)	Provide mechanisms for secure and, where applicable, automatic distribution of updates.	VDPT	Partial
CRA	Annex I, Part II, point (8)	Disseminate security updates without delay, accompanied by advisory information.	RMCM	Partial

Appendix C - Initial AENAON Requirements Baseline

Purpose and interpretation

This appendix consolidates the initial AENAON requirements baseline derived from the reference offshore wind use case, the threat-landscape analysis, the stakeholder questionnaire, the identified attack-surface and dependency characteristics, the impact analysis and the regulatory review presented in this deliverable. It addresses the D2.1 requirement to provide a list of requirements relating to preparedness-support services, relevant regulation and the cyber-range-based training programme.

The requirements are intentionally expressed at service and capability level rather than at individual tool or partner level. This reflects the federated nature of AENAON and preserves flexibility regarding the technical component or combination of components ultimately used to fulfil a requirement. Potential coverage is therefore mapped to the five AENAON preparedness-service areas: Digital Twins & Virtualisation Services (DTV), Vulnerability Discovery & Penetration Testing Services (VDPT), Security Awareness & Cyber Range Services (SACR), Threat & Risk Assessment Services (TRA), and Risk/Threat Monitoring & Cyberattack Management Services (RMCM).

The requirements constitute an initial M8 baseline rather than a final system specification. They are derived from the evidence currently available in D2.1 and should be reviewed and refined through T2.2 and T2.3, including further stakeholder engagement, towards the M10 use-case and requirements specification milestone. A service-area mapping denotes potential AENAON support and does not imply that a single service is solely responsible for implementation. Similarly, regulatory-support mappings indicate preparedness, assessment, validation or evidence-generation support and do not transfer or discharge legal obligations from the relevant regulated entity or other duty bearer.

Requirements taxonomy and service-area mapping

The baseline is organised into three categories aligned with the scope of D2.1:

- **PREP -** Preparedness Support Service Requirements
- **TRN -** Cyber Range & Training Requirements
- **REG -** Regulatory-Support Requirements

The service-area abbreviations used in the mapping are:

- **DTV -** Digital Twins & Virtualisation Services (T3.1)
- **VDPT -** Vulnerability Discovery & Penetration Testing Services (T3.2)
- **SACR -** Security Awareness & Cyber Range Services (T3.3)
- **TRA -** Threat & Risk Assessment Services (T3.4)

- **RMCM -** Risk/Threat Monitoring & Cyberattack Management Services (T3.5)

The mapping indicates an initial potential service-area coverage but will be further elaborated on and defined as the project progresses.



Initial requirements baseline

ID	Initial requirement	Principal D2.1 evidence / driver	Potential AENAON service-area coverage
PREP-01	The AENAON environment shall support identification and representation of relevant IT, OT and cyber-physical assets and the operational dependencies between them.	§2.3-2.4; §3.2; §6	DTV, TRA
PREP-02	The AENAON environment shall support representative modelling or virtualisation of offshore wind infrastructure, including relevant network segments, SCADA/ICS components, communications pathways and external stakeholder interfaces.	§2.3-2.4	DTV
PREP-03	Preparedness services shall support identification and contextualisation of known vulnerabilities affecting relevant software, firmware, network and OT assets.	§1.5; §4; §6	VDPT, TRA
PREP-04	Preparedness services shall enable vulnerability exploitation and penetration-testing scenarios to be assessed within a controlled environment without exposing operational infrastructure to unnecessary risk.	§4.5; §7.3; §9.2	VDPT, DTV, SACR
PREP-05	The AENAON environment shall support assessment of remote-access and privileged-access pathways involving operators, OEMs, maintenance providers and other authorised third parties.	§3.2; §6.2-6.3	VDPT, TRA, RMCM
PREP-06	Preparedness services shall support identification and assessment of supplier, OEM and third-party dependencies, including the potential propagation of cyber risk through shared platforms, services and digital components.	§3.2; §4.4; §6.1-6.2	TRA, VDPT
PREP-07	Threat information shall be contextualised against the assets, vulnerabilities, dependencies and operating conditions of the offshore wind use case in order to support prioritised assessment.	§4-6; §8	TRA, RMCM

PREP-08	The AENAON environment shall support assessment of both individual asset risk and potential cascading or propagated consequences across interconnected cyber-physical and operational dependencies.	§4.4-4.5; §7.1-7.3	TRA, DTV
PREP-09	Preparedness services shall support monitoring of changes in risk, vulnerabilities, threats and attack-surface conditions so that evolving exposure can be identified and reassessed.	§6; §8.1-8.3	RMCM, TRA
PREP-10	The AENAON environment shall support detection, investigation and evidence collection for relevant cyberattack scenarios, including correlation between affected assets, vulnerabilities, threats and observed activity.	§4; §7; §8.4	RMCM, TRA
PREP-11	Preparedness activities shall support assessment of degraded-operation, containment, restoration and recovery scenarios, including loss of monitoring, remote control, supplier support or communications.	§4.3; §4.7; §7.1-7.3	DTV, TRA, SACR, RMCM
PREP-12	Preparedness scenarios shall support multi-stakeholder coordination where incidents affect operators, OEMs, maintenance providers, communications providers, traders, TSOs or other interconnected parties.	§2.3-2.4; §6; §7.2; §8.2	SACR, DTV, RMCM
TRN-01	The cyber-range training programme shall provide offshore-wind-specific scenarios derived from the threat types and attack pathways identified in D2.1 rather than relying solely on generic enterprise-security exercises.	§3-6; §9.2	SACR
TRN-02	Training scenarios shall represent relevant interconnected IT, OT, SCADA/ICS, communications, cloud and remote-access environments.	§2.3; §4-6	SACR, DTV
TRN-03	Training shall accommodate different participant roles and levels of technical expertise, including operational, cybersecurity, engineering and management stakeholders where relevant.	§1.3; §3.2	SACR
TRN-04	The programme shall support hands-on attack-and-defence exercises, including vulnerability	§4; §9.2	SACR, VDPT, RMCM

	assessment, penetration testing, detection and response activities.		
TRN-05	Training shall exercise incident handling across detection, assessment, containment, communication, recovery and restoration under degraded operational conditions.	§7; §8.4; §9.2	SACR, RMCM, DTV
TRN-06	The programme shall support compound, large-scale and cross-border scenarios involving interdependent systems and multiple stakeholder organisations where appropriate.	§7.2; §8.2; §9.2	SACR, DTV, TRA
REG-01	AENAON services shall support assessment and evidence generation relevant to NIS2 cybersecurity risk-management obligations, including risk analysis, incident handling, continuity, supply-chain security and effectiveness assessment.	§2.2; §8.4; Appendix B	TRA, RMCM, SACR
REG-02	AENAON services shall support incident assessment and evidence collection relevant to NIS2 notification and reporting workflows, including severity, impact, indicators, mitigation and cross-border considerations.	§2.2; §8.4; Appendix B	RMCM, TRA
REG-03	Where products with digital elements fall within scope, AENAON services should support assessment or validation activities relevant to CRA product-security, vulnerability-management, component-transparency and lifecycle-security expectations.	§2.2; §8.4; Appendix B	VDPT, TRA, RMCM
REG-04	Where cybersecurity incidents involve personal data, AENAON-supported workflows should enable preservation of relevant evidence and incident information needed to support GDPR breach assessment and response by the responsible organisation.	§2.2; §4.2-4.3; §8.4	RMCM
REG-05	Where AI-enabled capabilities within the use case fall within applicable AI Act requirements, preparedness and validation activities should support relevant cybersecurity, robustness, human-oversight, logging and risk-management considerations.	§2.2; §4.8; §8.3-8.4	TRA, RMCM, SACR

REG-06	Where Data Act obligations are relevant to operational data generated by connected products and related services, AENAON-supported data exchanges should preserve appropriate access control, confidentiality, traceability and secure sharing between authorised stakeholders.	§2.2; §2.3-2.4	DTV, RMCM
REG-07	Regulatory-support functions shall maintain traceability between applicable legal obligations, relevant risks or scenarios, supporting AENAON service areas and the evidence generated through preparedness activities.	§2.2; §8.4; Appendix B	TRA, RMCM, SACR

Review and refinement process

The requirements above are intended to provide a traceable starting point for partner and stakeholder validation rather than to freeze the detailed implementation of the AENAON service stack. During T2.2 and T2.3, partners should confirm the wording, completeness and relative priority of the requirements, identify any additional sector-specific needs, and refine the service-area coverage where necessary.

Subsequent technical specification and customisation activities may decompose individual requirements into more detailed functional, non-functional, interface, data, security and validation requirements. Such decomposition should preserve traceability to the initial requirement identifiers defined in this appendix so that the evolution from D2.1 findings to the M10 specification and later preparedness-service implementation can be demonstrated.

Where Appendix B provides more detailed legal-obligation mappings, those mappings should be read as complementary to the REG requirements above. Appendix B provides article-level legal traceability, whereas Appendix C captures the service- and preparedness-level requirements derived from the overall D2.1 evidence base.

AENAON

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Partners

Asfalys

CILIX

Circular Economy Foundation

CYPRUS ORGANISATION FOR STANDARDISATION

Endoscope

more energy

PRIVACT

SIEMENS

Wind EUROPE

Zelus

EU-iNSPIRE
Centre of Excellence

MULTIMARINE
TRUSTED SEANERGIES