Sustainable Marine Structures
https://journals.nasspublishing.com/index.php/sms

ARTICLE

Ensuring the Security of Onshore and Offshore Wind Farms in the Context of War or Terrorism

Glib Ivanov [1*] ***, Yurii Poita*** [2*]

[1] *Department of Engineering Science and Ocean Engineering, National Taiwan University, Taipei 106319, Taiwan*
[2] *Department of Political Science and Political Technologies, Al-Farabi Kazakh National University, Almaty 050040, Republic of Kazakhstan*

ABSTRACT

Traditional fossil fuels powerplants and their supply logistics are easy targets compared to renewables – therefore renewable energy is paramount to securing energy resilience. While wind farms exhibit vulnerabilities, they provide a great measure of power generation distribution across a vast area. This paper analyses the problems of ensuring the security of wind power plants (both onshore and offshore) in relation to military threats – missile and aviation strikes, sabotage or cyber-attacks. The article is based on the study of cases of damage to wind power plants, an analysis of their vulnerable points, and computer modelling using the AQWA diffraction motion response analysis program. The research has shown that wind power plants have some vulnerable points. Onshore installations being structurally more resistant to potential military strikes, and their cables are already hidden underground. Offshore turbines, particularly floating, exhibit more Particularly floating wind turbines' mooring lines and cables already often fail naturally, making them easy targets for sabotage. The cost of currently available risk mitigation measures ranges from 6.71% of total wind farm cost for land-based turbines to 12.72% for a floating wind farm. Additional technological and organisational measures should be implemented to increase the resilience of wind power systems in times of war. These solutions must be cost-effective to justify their deployment in times of peace.

Keywords: Offshore Wind; Wind Energy; Military Conflict; Energy Independence; Infrastructure Security; Cyber Security

*CORRESPONDING AUTHOR:
Glib Ivanov, Department of Engineering Science and Ocean Engineering, National Taiwan University, Taipei 106319, Taiwan; Email: f10525106@ntu.edu.tw; Yurii Poita, Department of Political Science and Political Technologies, Al-Farabi Kazakh National University, Almaty 050040, Republic of Kazakhstan; Email: yuriipoita2@gmail.com

ARTICLE INFO
Received: 17 March 2025 | Revised: 3 April 2025 | Accepted: 23 April 2025 | Published Online: 9 May 2025
DOI: https://doi.org/10.36956/sms.v7i2.1865

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

1. Introduction

The Russo-Ukrainian war has highlighted the acute need to protect critical infrastructure, including energy systems, which during the conflict have been targeted with missiles, bombs, artillery strikes, and strike drones. Maliarchuk, Danyk and Briggs [1] explored the methods and effects of cyber and hybrid attacks on energy infrastructure in Ukraine, showing the potential of terrorist actors to disable power supplies without formal aggression. As deliberated by Farell, Zerriffi and Dowlatabadi [2], traditional fuel or nuclear energy infrastructure, in the context of military threats, has revealed the following drawbacks: a) the concentration of large generation capacity in one location, which significantly simplifies its destruction or damage during war or a terrorist attack; b) dependence on regular supplies of fuel/gas/coal, the availability and price of which depend on the global market, where the aggressor state may hold a significant share and influence over supplies.

While today's concentrated fossil fuel infrastructure is an easy target, dispersed renewable energy sources such as wind farms are being developed to replace them. As they contribute an increasingly greater share of energy production, they will inevitably become targets during conflicts in the near future.

In the context of increasing the survivability of energy systems and ensuring stable energy supply, and consequently national security, alternative energy sources have a number of advantages: a) geographical dispersion of power plants over distances, which prevents the loss of the entire generating capacity as a result of several point strikes; b) independence from fuel supplies, market price fluctuations, and operational autonomy (except for preventive maintenance). Current recommendations for Ukraine's post-war rebuilding of energy infrastructure are to focus on resilient and decentralised renewable energy sources [3].

A study by Binetti [4] on the post-war recovery of several countries showed that the re-development of destroyed energy infrastructure gave a sizeable boost to the manufacturing sector. Moreover, learning the lessons of war in Ukraine, Norwegians are becoming supportive of new land-based wind turbine development, when they were traditionally opposed to them [5].

At the same time, renewable energy sources also have vulnerable points that must be taken into account in order to reduce the threat of missile and air strikes. While hydropower dams and solar panels have been widely destroyed during the war in Ukraine, wind farms showed resilience. This paper aims to highlight the potential threats in the event of external interference with wind power plants and to provide recommendations for their protection during design, construction, and operation. The paper examines threats to both onshore and offshore wind turbines (fixed-bottom and floating), their typical scales easily seen from **Figure 1**. While 14–16 MW land-based wind turbines are being introduced, as of 2024, the average MW rating of newly installed land-based wind turbines was still short of 3.5 MW [6].

Ukraine has a successful example of the Tyligulska wind farm becoming the first one built in a warzone or during a war [7]. Currently, Ukraine only has land-based turbines, but it also has a noticeable offshore wind potential [8]. Other countries at conflict risk in Asia, the Middle East, and the Baltic also have significant offshore wind installed capacity or potential. This paper goes through different types of wind turbines and farm arrangements to determine which are best suited for the countries at risk of war or terrorism.

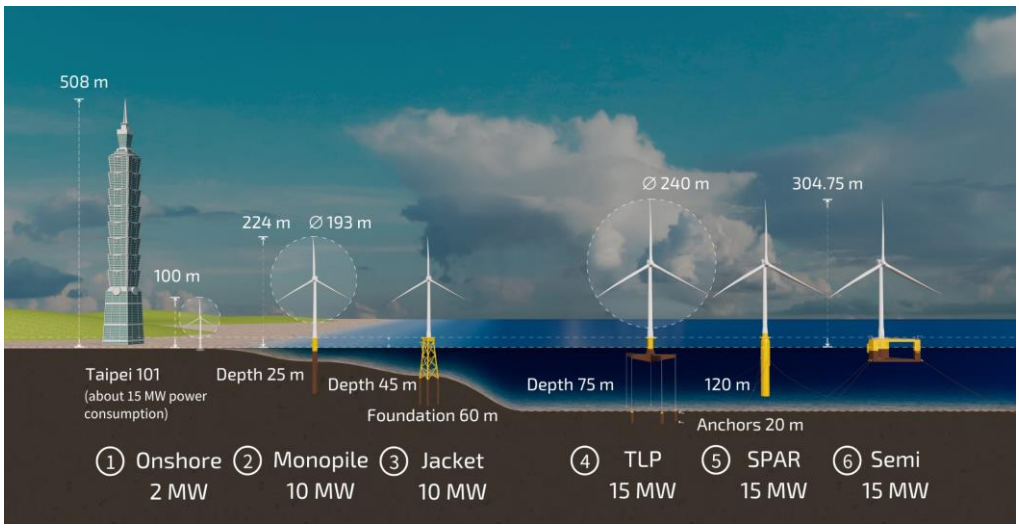


Figure 1. Different types of wind turbines and their typical scale.

Source: Picture courtesy of Prof. Kai-Tung Ma, National Taiwan University.

2. Methodology

This paper compares all 3 types of wind farms on their safety level, which is analysed component-wise for the tower, nacelle, foundation, cable and substation. While there is little data on damage by military action available, we can make educated guesses on the technology's weaknesses by analysing accident statistics. Risk and consequence are evaluated on a low-medium-high scale, where risk can be thought of the attractiveness of this damage for the potential attacker. A low consequence rating means the damage does not significantly impact the farm operation or the damage can be easily fixed; medium consequence is either serious but repairable damage to the whole farm or fatal damage to a single unit, while high consequence means potential fatal damage to the whole wind farm.

Where possible, suggestions are provided to increase safety, and their potential cost impact is estimated as a percentage increase in overall wind farm cost. For consistency, all 3 types of wind farms' cost structures come from the US National Renewable Energy Laboratory 2024 Cost of Wind Energy Review [6]. This report treats all installation activities as a lump sum without differentiating for cable installation, foundation installation, etc., and it also mentions that installation cost has much higher contingency as compared with more predictable capital cost, so only capital expenditure cost increase is considered in the mitigation cost for the purpose of this paper. Individual turbine and nacelle parts cost breakdown is assumed from Lilas et al. [9]. Onshore substation cost of all wind farm types is assumed to be the same for fairness and taken from [10].

For the assessment of floating wind turbines, the semi-submersible type is chosen as it is both the most widely used type around the world, as well as there exists a detailed structural model developed, which is necessary for detailed analysis. The floater "TaidaFloat" is analysed using a programme AQWA to find out what it takes to sink it. Floater's key parameters are shown in **Table 1**.

Table 1. Floater principal characteristics.

Length	81.6 m
Breadth	94.2 m
Height	35 m
Draught	22 m
Total displacement	±20, 300 t
Hull weight	4002 t
CG height	17.35 m from BP
Coordinates origin	Pontoon centroid at base plane (BP)

AQWA employs linear potential flow theory to predict the dynamic response of floating wind turbine platforms under various wave conditions. In our case, the method solves Laplace's Equation (1), for the velocity potential Φ, subject to boundary conditions on the free surface and the floater's wetted surface. The computed hydrodynamic forces are then used in the equation of motion (2).

$$\nabla^2 \Phi = 0 \tag{1}$$

$$M\ddot{x} + C\dot{x} + Kx = F \tag{2}$$

where M, C, and K are the mass, damping, and stiffness matrices, respectively, and F represents the wave-induced force.

A geometric model is constructed and fed into AQWA, which solves the above equations and simulates the platform's motions (e.g., heave, roll, pitch, and sway). This analysis allows us to determine critical thresholds, such as the wave height at which one or two compartments flood, thereby informing design modifications to enhance safety and stability.

3. Onshore Wind

To understand potential weaponized strikes' impact, accidents leading to similar damage can be analysed. Most accidents at wind turbines occur due to various damages to electrical equipment and blades, and although such damages can disable the turbine, they can often be quickly repaired. At the same time, a large-scale fire or the collapse of a tower makes further repair of the wind power plant impossible [11].

A tower collapse can occur for several reasons, including strong winds, damage to the tower bolts, or a blade striking the tower due to deformations in the blade. The turbine tower is made of sheet steel with internal stiffening ribs, and there are experimental variants with a lower part made of concrete. The metal thickness ranges from 30–50 mm at the base to 20 mm at the top; parts of varying thickness are usually connected by flanges with bolts, as seen in **Figure 2** [12].

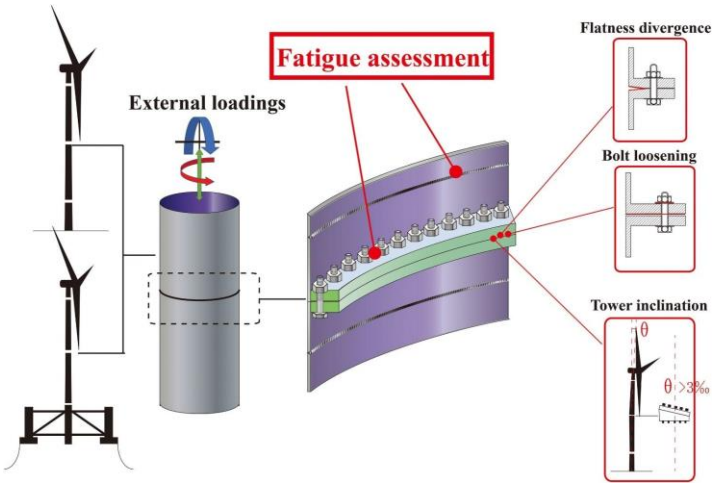


Figure 2. Structure of the wind turbine tower with a flanged connection and common problems (similar for onshore and offshore turbines) [12].

Statistics show that most tower collapses occur due to bolt damage (resulting from excessive wind force or poor fastening). According to a study by Chou, Ou and Lin [13], in various wind turbine models, bolt damage occurred in 82% of cases at the junction between the lowest and second levels, that is, at approximately 25% of the height from the bottom, as seen in **Figure 3**. This is the weakest point of the tower, which should be reinforced to protect against projectiles.

Another threat may be the onset of a fire in the nacelle (see **Figure 4**), which consists of a cast iron platform connected to the tower, on which the generator base, transformer gearboxes, and auxiliary devices are installed. The nacelle walls do not bear any load and are made of thin steel, which can be easily damaged, for example, by a UAV (Unmanned Aerial Vehicle) strike. At the rear, the wall has openings for cooling and ventilation.

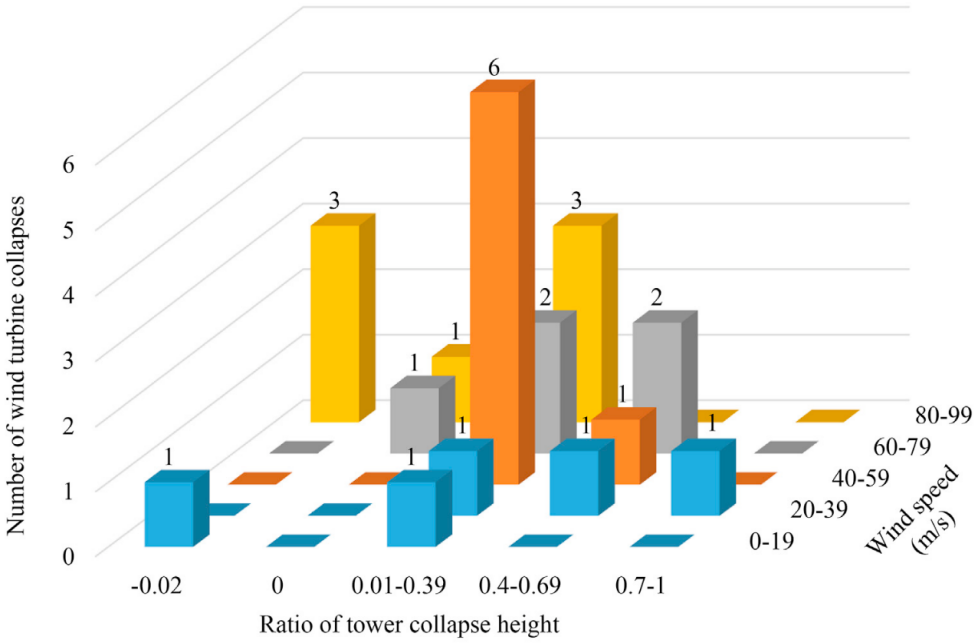


Figure 3. Statistics of tower collapse depending on the fracture height and wind speed [13].

Figure 4. Consequences of a fire in the turbine nacelle – a destroyed nacelle on a V150-4.2MW Vestas turbine at the 164MW Myrnenska wind farm in Ukraine [7].

According to Uadiale et al. [14], approximately 10%–30% of turbine damages are caused by fires, and fires are the second most common case of non-repairable damage. In addition to the possibility of a short circuit causing the fire, there are three flammable liquids in the nacelle, as listed in **Table 2**.

Table 2. Flammable liquids in the nacelle.

Liquid	Boiling Point (°C)	Ignition Temperature, Ti (°C)	Operating Temperature, To (°C)	Ti–To (°C)
Machine oil	300	170–225	95	75–130
Hydraulic fluid	-	148–315	100	48–215
Transformer oil	300–400	140	105	35

Source: Adapted from Yu [15].

These liquids are constantly at high operating temperatures, so in the event of a slight temperature increase, there is a high probability of a fire. In the event of external damage to the transformer (for example, because of a UAV strike), the difference between the operating temperature of its oil and the ignition temperature is the smallest, i.e., there is a high probability of it catching fire or exploding. Depending on its age and manufacturer, the nacelle may be equipped with a fire protection system of varying quality. Possible mitigation is switching to a dry-type transformer, which is about 30% more expensive [16].

In addition to the transformer, liquid is also present in the hydraulic cylinders that provide blade pitch control (Pitch Control System). Unlike all other parts, these are not located in the nacelle but in the rotor – at the front part of the wind turbine (see **Figure 5**). Damage to these cylinders, even if it does not cause a fire, will at the very least prevent the adjustment of the blade pitch, which protects the turbine during strong storm winds. This will lead to serious damage to the generator or the destruction of the wind turbine due to a blade striking the tower (caused by bending).

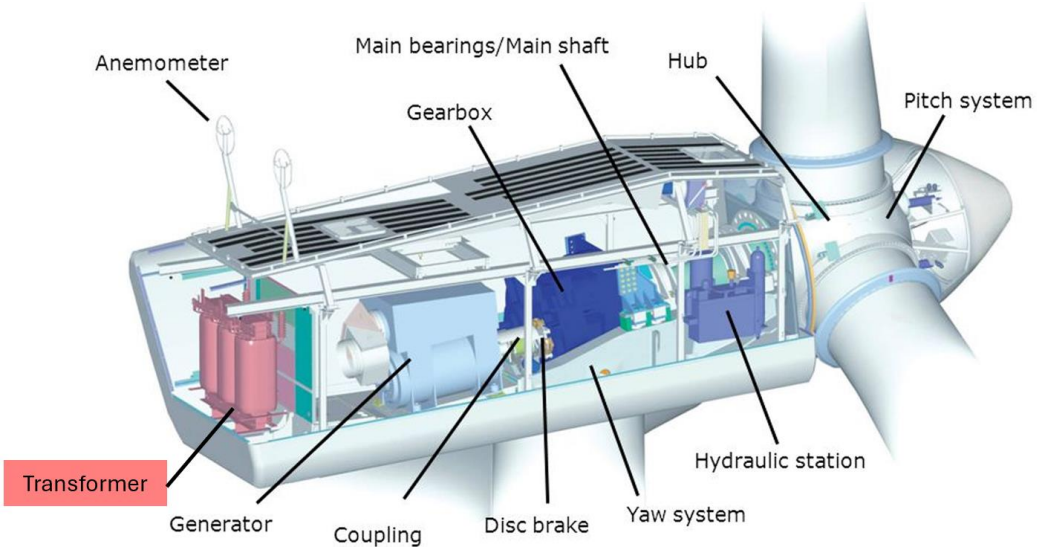


Figure 5. Schematic of the nacelle of a typical Vestas wind turbine.
Source: Adapted from Garidis [17].

Furthermore, depending on the temperature regime of the area, the nacelle is equipped with a heating and cooling system (for regions with possible sub-zero temperatures) or a cooling and dehumidifying system (in humid and warm regions). Damage to these systems will lead to the gradual failure of the wind turbine.

In this context, the wind turbine may face threats from UAVs, although only those with sufficient engine power to counter the turbulent airflow generated by the blades. In particular, UAVs have begun to be used for visual inspection of turbine damages; obstacle avoidance arose as one of the critical concerns as these systems developed [18]. This is only safe when the blades are not moving: the operation of the turbine creates a turbulent airflow around and behind the blades, where the speed and direction of the air change abruptly every second [19], as seen in **Figure 6**. Therefore, small UAVs (for example, of the Mavic type) are unable to cope with such sudden and strong changes and fly in an unpredictable direction, risking collision with the turbine or a fall. At the same time, more powerful UAVs can overcome the air turbulence.

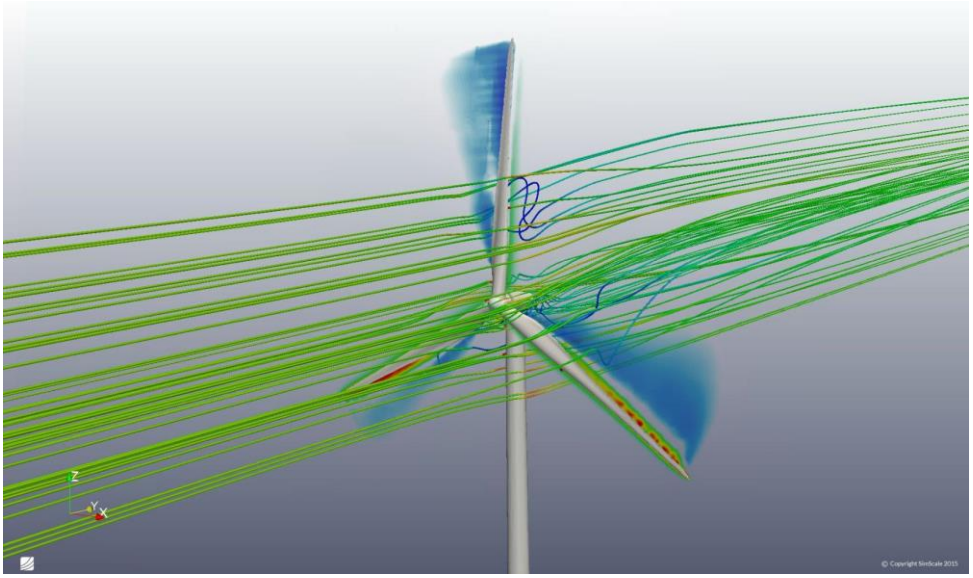


Figure 6. Airflow past a turbine [19].

In view of the above, despite the large size of the turbine, causing significant damage is difficult. The tower itself can withstand significant loads and continue to operate after sustaining damage. The most vulnerable part of a wind power plant is the nacelle at the top of the tower, which houses sensitive equipment and flammable liquids. Consequently, to protect the nacelle, an anti-drone protective “screen-grid” can be installed

on the sides and above. **Table 3** summarises the risk and mitigation costs.

Table 3. Summary of risks and mitigation costs for land-based wind turbines.

Component	Risk	Risk	Consequence	Mitigation	Approximate Mitigation Cost, % Increase of Total Farm Cost
Tower	Projectile hit	Low	Medium	Reinforce critical 1/3 tower section by 50% thickness	1.57
Nacelle	Fire due to firearms hit	High	Medium	Change transformer from oil to dry type	0.45
Nacelle	Fire/explosion due to UAV attack	Medium	Medium	Install anti-UAV mesh grid.	0.25
Foundation	Explosion	Low	Medium	Not needed	-
Cable	None	-	-	-	-
Onshore substation	Targeted attack	High	High	Underground substation	4.69
				Total	6.71

4. Fixed-Bottom Offshore Wind

An offshore wind turbine consists of three main parts, as shown in **Figure 7**:

- Turbine – the power and dimensions of which are one and a half to three times larger than those of an onshore turbine. For this reason, and to avoid destructive resonance, the thickness of the steel pipe (tower) is 40–60 mm, making it highly resistant.
- Transition piece – a cast iron (or sometimes welded steel) component on which the tower is mounted; it is very robust. Unlike onshore turbines, electrical devices, including the transformer, can be located in it rather than at the top, which makes them more protected.
- Foundation (a single pipe or steel structure) – the part that is embedded in the seabed or connects the tower with piles. It bears the weight and moment of the turbine and the loads from waves and currents, thus it is extremely sturdy, with metal thickness ranging from 40 to 150 mm.

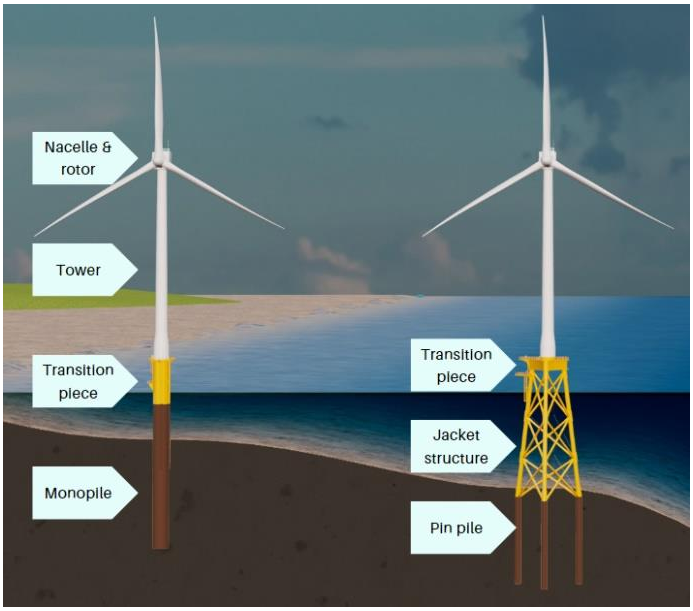


Figure 7. Main parts of an offshore wind turbine.

In this regard, the above-water part of an offshore wind turbine is very robust and resistant to damage. The threat in the event of military action lies in the inability to rebuild or perform a major repair on the wind turbine during wartime. Given the technical characteristics of the turbine, such operations are carried out by specialised vessels, such as a Jack-Up (see **Figure 8**), which rest on the seabed and use a crane to install or replace components, most often the damaged blades of the turbine or equipment in the nacelle [20].

By comparison, operations for onshore turbines are carried out by widely available cranes on truck- or crawler-mounted platforms, and the nacelle of the largest turbines weighs no more than 400 tonnes (with the turbine height being 120–140 m). Meanwhile, the largest offshore turbines have nacelle weights exceeding 1000 tonnes (with the turbine height reaching up to 280 m) [21], and worldwide there are no more than approximately 10 vessels capable of performing such operations. These vessels are bulky, remain stationary during operations, and can be easily targeted by missile or other means. Since there is high demand for these vessels, their owners are reluctant to carry out works in conflict zones.

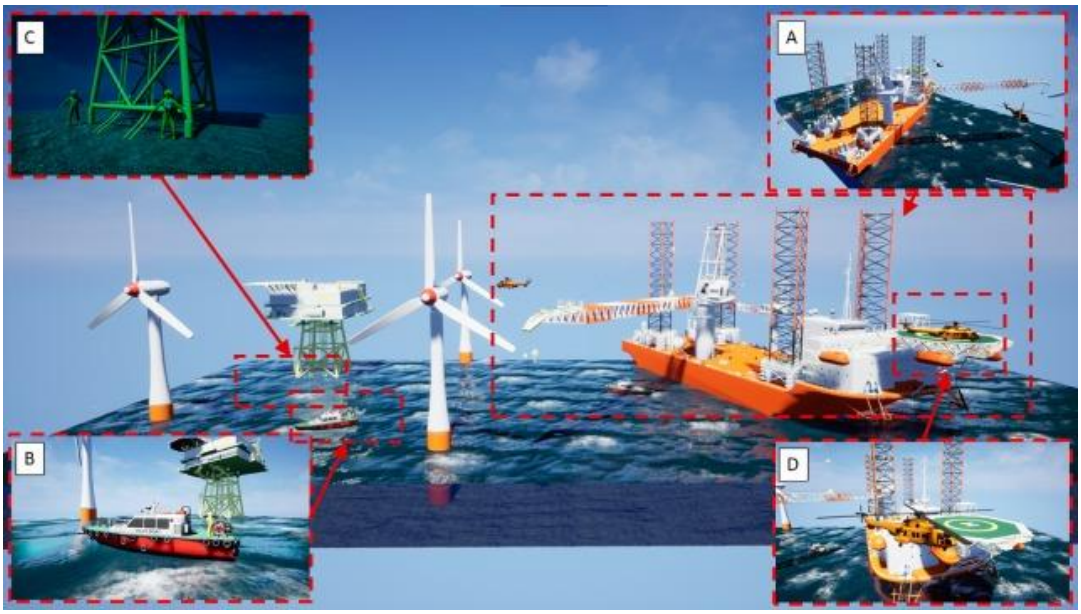


Figure 8. Jack-up vessel performing and other support vehicles for turbine installation and maintenance. Source: From Mitchell et al. [20].
Note: A – Jack Up crane vessel; B – crew transport vessel; C – subsea pipeline and cables installation divers; D – support helicopter.

Substantially more vulnerable is the submarine cable. According to leading offshore wind classification body Det Norske Veritas, 80% of claims for offshore wind turbine insurance are related to problems with subsea cables [22]. The cable can be of two types: an internal cable, which connects one wind turbine to a neighbouring turbine; and an export cable, which connects the last turbine in a chain to an onshore substation, or an offshore substation with an onshore one (see **Figure 9**).

Cable damages occur due to the following factors [23]: human errors during connection; incompatibility of the standard cable with local conditions and the type of support, etc. However, in the context of human intervention, the main cause of cable damage in the underwater section is damage by a fallen ship anchor [24] or damage by the fishing net guides of fishing vessels, including deliberate actions by fishermen or Special Operations Forces. Repeated cable damages related to vessels, as well as cases of power outage due to such damage, demonstrate the technical feasibility, and even ease, of such interference [24,25]. Since 2013, there have been at least 11 cases of undersea cable damage around Taiwan and at least 11 such incidents in the Baltic Sea – areas with existing large-scale offshore wind developments [26]. Special devices have been developed to ease the destruction of cables [27].

In order to protect the cable from such damage, it is now being buried underground, which complicates its visual identification, as in **Figure 9**. When repair or inspection is necessary, knowing the approximate location of the cable on the map, it is located on site using marine drones equipped with specialised sonar. Due to natural factors, over time, sections of the cable may surface on the seabed, at which point they are covered with stones. Since companies involved in the laying of submarine cables may have connections with governments that might be interested in damaging

cables or sabotage, it is advisable to choose a contractor taking into account geopolitical risks, as the contractor will be familiar with the configuration and location of the cable routes. The range of possible prices of subsea cables based on actual data is given in reference [28]; assuming the cheapest option as potentially dangerous and the most expensive option as the safe one, the markup for using the safe option vs cheap would be 76.5%.

Submarine cables usually do not run in a straight line but have many bends to avoid problematic areas of the seabed. Even in the absence of the aforementioned difficulties, the cable route should be made more complex to complicate its location by the enemy. Information about the cable route is carried on maps to avoid hazards and allow planning of adjacent and intersecting cables (including telecommunications).

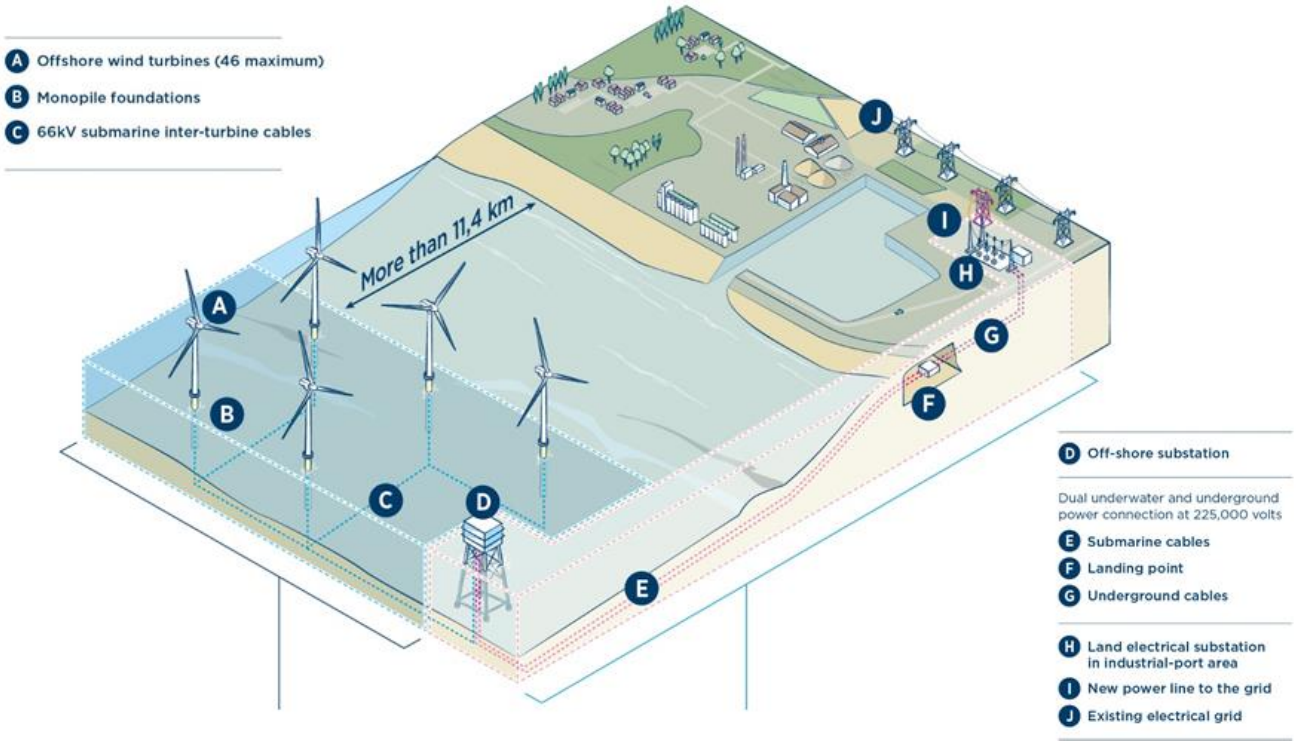


Figure 9. Schematic of Dunkirk offshore wind farm with underground cable.
Source: Courtesy of Dunkerque Wind Park [29].

With regard to the security of the substation, **Figure 10** shows four possible electrical schemes for offshore wind power plants, each with a different level of survivability against being taken out of service:

- Without a substation. A small wind power plant, such as one located close to the shore, usually does not have a substation, and the turbines are connected directly to the grid. This is the rarest and safest scheme because the substation is a vulnerable element, the loss of which would lead to the malfunctioning of the wind power plant. Such a wind power plant may suffer significant voltage losses.
- Single substation. Small cables from all strings, or from individual wind turbines, are connected to a substation, from which a high-voltage cable runs to the onshore electrical network. If the substation is offshore, it can be located in the centre of the wind farm to reduce transmission losses. This is the most common scheme, which minimises voltage losses, but from a military threat perspective, it is the most dangerous due to the presence of a single vulnerable node.
- Dual substations. Wind turbines are arranged in one or several long strings, interconnected by cables; loop cables allow both substations to be used by all the turbines in case of either substation's failure.
- Independent cables run from both ends of the string to two substations located far apart (or to oil platforms – energy consumers). In the future, these might also be two export substations (considering interconnections between countries).

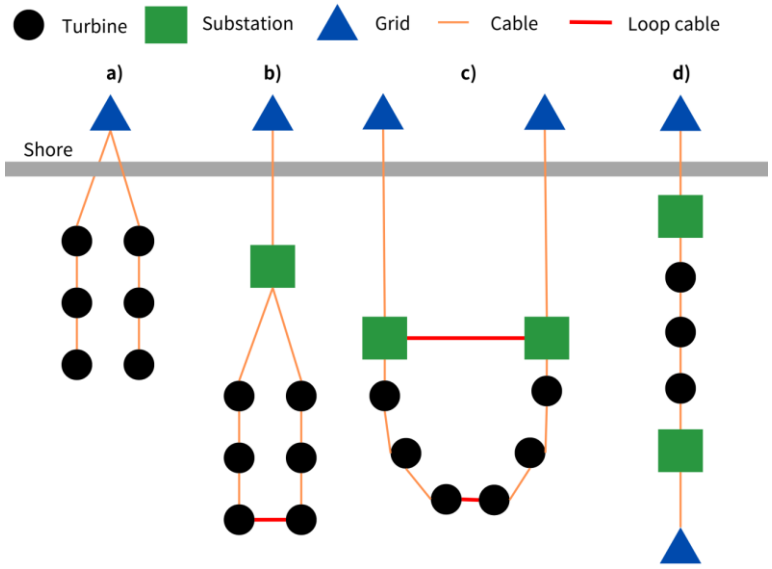


Figure 10. Wind farm schemes.

The export cable of an offshore wind power plant can run either to an offshore or an onshore substation, depending on the distance and water depth. The offshore substation is a large and vulnerable object, but it can significantly reduce energy transmission losses, while an onshore substation could be concealed.

Thus, submarine cables can be easily damaged if their exact location is known. To ensure greater security, it is advisable to: a) complicate the cable route to reduce the likelihood of the enemy locating the cable; b) restrict public access to cable maps; c) hire vessels for the installation and repair of cables, taking into account geopolitical risks to maintain the confidentiality of cable routes. Regarding substation security, which is the weak link whose damage would de-energise the entire wind power plant, it is recommended to use two onshore substations completely buried underground with concrete protection. Unfortunately, the exact cost hike of moving the substation underground could not be easily determined, as there are many factors involved; the only available reference estimated that a 115 kV (similar to offshore wind farms) underground transmission would cost 73% more than an above-ground facility; thus, this number is adopted as a raw estimate [30]. **Table 4** summarises the risk and mitigation costs.

Table 4. Summary of risks and mitigation costs for fixed-bottom offshore wind turbines.

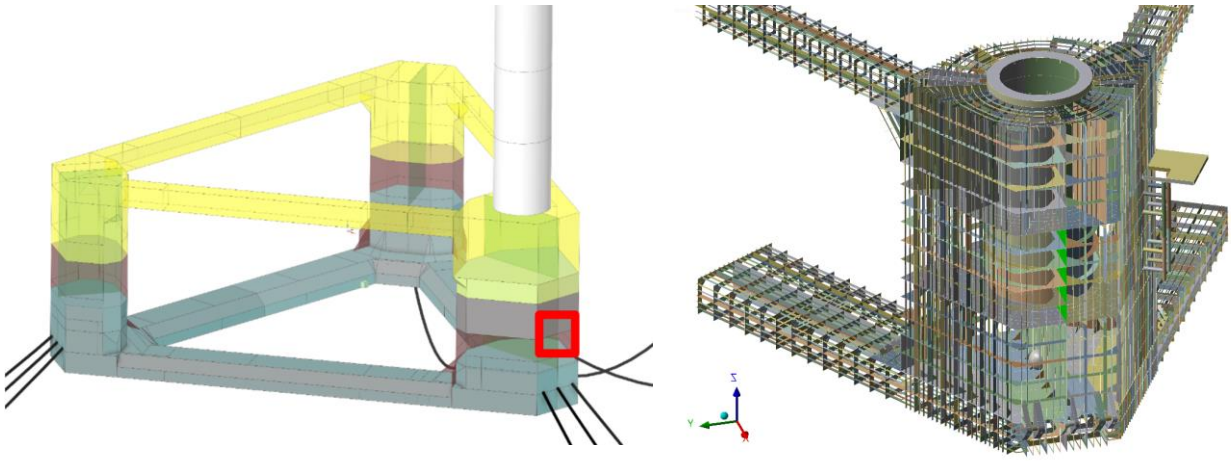
Component	Risk	Risk	Consequence	Mitigation	Approximate Mitigation Cost, % Increase of Total Farm Cost
Tower	Projectile hit	Low	Low	Not required	-
Nacelle	Fire due to firearms hit	High	Medium	Change transformer from oil to dry type	0.26
Nacelle	Fire/explosion due to UAV attack	Medium	Medium	Install anti-UAV mesh grid.	0.14
Foundation	Explosion	Low	Medium	Not required	-
Cable	Sabotage	High	High	Supplier management	2.35
Offshore substation	Targeted attack	High	High	Onshore substation/double substation	Power loss/3.25
Onshore substation	Targeted attack	High	High	Underground substation/ double underground	1.1/2.19
				Total	3.85 – 8.19

5. Floating Offshore Wind

Due to measures taken to prevent vibrations caused by sea waves, the turbine tower installed on a floating wind turbine is thicker (amounting to 50–70 mm) than that of a fixed turbine, which makes it highly resistant to impacts.

At the same time, there may be difficulties in ensuring the security of the floating platform to which the tower is attached. A floating platform can be of various types such as Spar, Semi-Submersible, and TLP, but its capabilities are limited by factors such as water depth, maximum wave height, wind speed, and current. In most environments, semi-submersible platforms with several columns are preferred. In that case, it is easy for a missile or drone to hit the platform due to its broad profile, although most platforms contain several columns [31,32]. The width of a column may be 5–15 metres, which also makes it an easy target for a marine drone or missile.

At the same time, according to classification society rules, floaters, like ships, must be divided into many compartments, so that in the event of complete flooding of any 1 (or more) compartment(s), the platform remains afloat. If water reaches openings on the deck (hatches, ventilation pipes, etc.), the platform may sink. **Figure 11** illustrates the division of the TaidaFloat platform into compartments and the hull stiffeners under the outer shell. The most dangerous area for damage is the middle of the main column at the waterline – if it is damaged and the internal bulkhead is bent, water will immediately enter two large compartments; however, for this to occur, the impact must be precisely in the centre of the main column, which is a more difficult task.



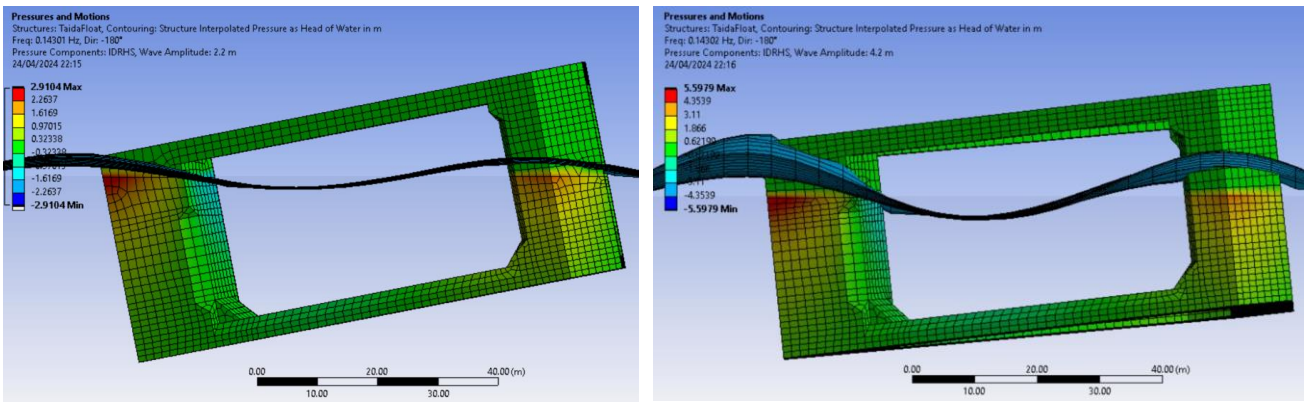
(**a**) (**b**)

Figure 11. (**a**) Division of the platform into compartments. The lower compartments are filled with ballast water, and two compartments in the central column are flooded due to a hit in the critical location (red square). (**b**) Example internal stiffener arrangement of TaidaFloat, the critical bulkhead is highlighted in green.

Two scenarios of such damage were investigated using a diffraction motion response analysis program: flooding of one compartment and flooding of two compartments. The goal is to find out the wave height that will flood the deck when the floater is tilted due to flooded compartments; the probability of this wave height can be easily determined for any sea region.

If two compartments are flooded due to structural damage, in calm conditions or light wind, waves of average height (4.4 m) are tall enough to keep flooding the deck and sink the floater. Any significant wind significantly lowers this threshold, easing the sinking, as evident from **Figure 12**.

In the case of flooding of only one compartment, flooding by waves is unlikely; however, if the damage happened during a storm or strong wind, flooding is probable. Thus, the platform can be flooded by one or two precise missile or seaborne drone strikes with a piercing capability of 15–20 mm of steel. Flooding of the platform will not lead to damage to neighbouring platforms.



(**a**) (**b**)

Figure 12. Floater motion response in AQWA. (**a**) Two compartments flooded. The deck is flooded at a wave height of 4.4 m (wave period – 7 s). (**b**) One compartment flooded. The deck is flooded at a wave height of 8.4 m (wave period – 7 s).

The mooring system could be another vulnerable point. A floating wind turbine is held in place by anchors connected to the platform with mooring lines: steel chains (diameter 100–200 mm) in shallow waters (up to 100 m depth), or chains with an inserted synthetic elastic rope (diameter 100–300 mm) in deep waters (100+ m) [33].

Typically, the mooring system is designed such that if any one line is damaged, the platform remains in place and operational. In practice, this means that the platform does not drift far even if several lines are damaged, but its electrical cable will be damaged, taking it out of the grid.

If all (at once) or a critical number of lines (during a storm) are damaged, the platform will begin to move under the influence of waves, wind, and currents, which in conditions of close proximity [34] within a floating farm is likely to lead to damage to other platforms or their cables and mooring lines [35]. For this reason, the most dangerous impact is on platforms in the centre of the farm.

The steel chains with a diameter of 100–200 mm [36] used for such lines are extremely strong and even capable of damaging vessels. Being barely visible and underwater, they are resistant to ballistics but can be cut by divers. Synthetic ropes are much weaker and are considered to be susceptible to damage after any forceful contact with rocks, vessels, or fishing trawls.

Another underwater part is the dynamic power cable, which goes from the floater and connects with the buried power cable on the seabed. Any forced loads, including those caused by excessive platform movement or collision with mooring lines, will lead to its damage. Nonetheless, it is very mobile and a barely noticeable underwater target. The cable not only transmits the turbine's energy to the grid but also supplies energy to maintain the turbine's internal systems, such as ventilation, surveillance cameras, system sensors, and navigation lights. In the event of its damage, an alternative power source should be available; usually, in such cases, a temporary fuel generator is delivered to the platform.

The substation in floating wind power plants is the same as in fixed ones, with the difference that an offshore substation can also be floating. In this case, it will be exposed to the same risks (flooding, drifting, de-energisation) as the floating wind turbine.

Thus, a floating platform can be easily sunk as a result of a missile or waterborne drone strike. To increase the survivability of floating wind power plants, it is advisable to design platforms with a smaller waterline area and division into a greater number of compartments. Damage to the mooring system of one platform may trigger a chain reaction and damage many platforms, as they are very tightly packed in the wind farm area [34].

To avoid this, it is recommended: a) to use steel chains or ropes instead of synthetic ones, making them harder to cut; b) to allocate more lines to each platform; c) to increase the distance between platforms in the farm to prevent a chain reaction. **Table 5** summarises the risk and mitigation costs.

Table 5. Summary of risks and mitigation costs for floating offshore wind turbines.

Component	Risk	Risk	Consequence	Mitigation	Approximate Mitigation Cost, % Increase of Total Farm Cost
Tower	Projectile hit	Low	Low	Not required	-
Nacelle	Fire due to firearms hit	High	Medium	Change transformer from oil to dry type	0.21
Nacelle	Fire/explosion due to UAV attack	Medium	Medium	Install anti-UAV mesh grid.	0.12
Foundation	Sinking	Low	Medium	Increasing compartmentation	3.44
Mooring system	Sabotage by cutting	Medium	High	Using chains (standard for now)	-
Dynamic cable	Sabotage by cutting	High	Medium	Not possible	-
Static array cable	Sabotage by cutting	Low	Low	Supplier management	2.58
Static export cable	Sabotage by cutting	High	High	Supplier management	1.48
Offshore substation	Sinking	High	High	Double substation	2.71
Onshore Substation	Targeted attack	High	High	Underground substation /double underground	1.09/2.19
				Total	11.62/12.72

6. Cyber Security

The largest global certification provider for offshore wind, DNV, has released a new report in 2025, finding that: "Two in three energy professionals (65%) say their leadership views cybersecurity as the greatest current risk to their business." [37] What are those risks they are afraid of? The best examples might be Russian attacks on Ukrainian and EU's energy sectors in the last decade.

The cyberattacks that targeted Ukraine's power grid in 2015 and 2016 stand as a watershed moment in the history of cyber warfare, demonstrating the potential for digital intrusions to cause significant real-world consequences. In December 2015, a coordinated attack utilizing a version of the BlackEnergy 3 malware caused a power outage affecting nearly a quarter-million people for several hours [38]. This attack involved gaining remote access to SCADA systems, manipulating controls to shut off power at multiple substations, and even hindering restoration efforts by disabling some control equipment [39]. A year later, in December 2016, another more sophisticated attack occurred in Kiev, causing another unexpected blackout affecting approximately 225,000 customers [40]. This second attack employed a complex malware known as CRASHOVERRIDE (or Industroyer), which was specifically designed to directly interact with and manipulate industrial control systems used in electric grids. The attackers were able to cause breakers to trip at multiple substations, leading to the power outage, and also sabotaged management systems, requiring manual intervention to restore power. More recently, in late 2022, the Russia-linked threat actor Sandworm targeted a Ukrainian critical infrastructure organization, deploying OT-level living off the land techniques to trip substation circuit breakers, resulting in an unplanned power outage coinciding with widespread missile strikes [41]. These incidents collectively highlight the tangible risks of cyberattacks on critical energy infrastructure and the potential for widespread disruption of essential services.

Another major disruption happened to thousands of German wind turbines in 2022, linked to the ViaSat satellite hack, providing a compelling example of an indirect cyberattack with significant implications for the renewable energy sector. In February 2022, coinciding with Russia's invasion of Ukraine, a cyberattack targeted the KA-SAT satellite network operated by ViaSat, a major satellite internet provider [42]. This attack had a widespread impact, affecting various users across Europe, including approximately 5,800 wind turbines in Germany managed by the energy company Enercon [43]. The turbines relied on satellite communication via ViaSat for remote monitoring and control, and the cyberattack rendered this communication unavailable.

While the attack did not directly target the wind turbines' control systems [44], it effectively disabled the remote management capabilities, highlighting the vulnerability of critical infrastructure to attacks on third-party service providers. This incident underscores the importance of considering the entire ecosystem connected to wind farms, including communication providers, and ensuring that robust security measures are in place across all dependencies to prevent such indirect compromises.

Even traditional oil and gas infrastructure such as pipelines becomes prey to cyberterrorism enabled by control systems digitalisation [45,46].

Successful cyber intrusions targeting wind energy facilities present risks that extend beyond damage to individual turbines, potentially compromising the stability of the interconnected power grid [47]. As the penetration of wind power, an Inverter-Based Resource (IBR), increases, coordinated cyberattacks manipulating the power output of multiple turbines can induce significant supply-demand imbalances, leading to frequency and voltage instability [48]. Such instability is particularly pertinent given the operational characteristics of modern power systems with high IBR levels. Attacks targeting critical control systems, including those associated with High-Voltage Direct Current (HVDC) transmission links often used for offshore wind, could potentially initiate cascading failures throughout the grid [49].

6.1. Mitigation Strategies

A robust cybersecurity posture necessitates a multi-faceted defence-in-depth strategy, integrating security considerations throughout the system lifecycle.

Security by Design and Standardization (IEC 62443): Foundational security requires adopting "security by design" principles, guided by established frameworks such as the IEC 62443 series of standards. These standards provide requirements for Industrial Automation and Control Systems (IACS) cybersecurity across the lifecycle, addressing technical and procedural aspects for manufacturers, integrators, and operators [50].

Intrusion Detection and Prevention Systems (IDPS): Implementation of IDPS is crucial for monitoring network traffic and system activities to identify and counteract malicious actions or policy violations [51]. Advanced techniques, including machine learning algorithms, are being developed to enhance IDPS performance within Supervisory Control and Data Acquisition (SCADA) environments specific to wind turbines [51].

Network Monitoring and Anomaly Detection: Continuous network monitoring provides essential visibility. Anomaly detection techniques, including unsupervised machine learning methods, can identify deviations from baseline behaviour in ICS networks, potentially indicating novel threats or system [52].

Access Control and Vulnerability Management: Stringent access control mechanisms, incorporating principles like least privilege and strong authentication, are fundamental [53]. These should be complemented by regular vulnerability assessments and penetration testing to proactively identify and mitigate system weaknesses.

Organizational Measures: Cultivating a strong cybersecurity culture through continuous training and awareness programs is essential, as many vulnerabilities come from people unaware of how their actions facilitate attacks. Additionally, fostering robust information-sharing mechanisms among industry stakeholders and governmental bodies can improve collective defence capabilities, although strengthening the international cybersecurity culture in the electricity sector remains an ongoing need.

6.2. Specific Considerations for Offshore Wind

The offshore environment introduces distinct cyber-security challenges.

Communication Systems: Offshore wind farms depend heavily on complex communication architectures (e.g., satellite, subsea fiber optics) for remote operation and monitoring. Ensuring the security and resilience of these communication links, including managing risks associated with third-party dependencies, is paramount.

Substation and Transmission Security: Offshore substations serve as critical aggregation points and require dedicated cyber-physical security measures, considering both the substation automation systems and the high-voltage transmission infrastructure. Their remote nature increases the impact of certain attacks like denial-of-service.

Floating Platform Control Systems: Floating offshore wind turbines utilize sophisticated control systems for platform stability and station-keeping, introducing unique cyber-physical attack surfaces that must be addressed within security frameworks. The integrity of sensor inputs to these systems is particularly critical as shown by the Stuxnet worm [54]. Secure management of both remote and physical access for maintenance activities on offshore assets also necessitates rigorous procedures and CCTV monitoring.

7. Economic Impact of Attacks on Wind Farms

Recently, Taiwan's wind farms were affected by a targeted spying malware [55]. While the intents or

perpetrators are not entirely clear, it might be for further sabotage. To illustrate the potential economic impact of such sabotage, consider a hypothetical scenario where a coordinated physical and cyber-attack disables 30% of an offshore wind farm's capacity in Taiwan for a period of six months. Assume a large offshore wind farm with a total capacity of 1 GW (1000 MW). Disabling 30% would mean 300 MW of capacity is offline. Based on industry averages [6], the capital expenditure for offshore wind is around $5.4 million per MW. Thus, the initial investment for 300 MW could be around $1.62 billion. The net annual energy production for offshore wind can be around 3,300 to 4,300 MWh per MW per year. Assuming an average of 3,800 MWh per MW per year, 300 MW would typically generate 1,140,000 MWh per year, or approximately 570,000 MWh over six months. The average electricity price in Taiwan for industrial users in 2025 is around US$0.135 per kWh [56]. Therefore, the lost revenue over six months could be approximately 570,000 MWh * $135 per MWh = $76.95 million.

Repair costs for physical damage to multiple offshore turbines could be substantial. Assuming damage to key components like blades and potentially towers across 30% of the farm's capacity, the repair costs could easily range from tens to hundreds of millions of dollars, depending on the severity of the damage and is very difficult to estimate. For instance, replacing a single offshore turbine can cost upwards of $11 million [57]. If the attack necessitates the replacement of even a few turbines and major repairs to others, the total repair expenses could be significant.

The sudden loss of 300 MW of offshore wind capacity for six months would likely require Taiwan's grid operator, Taipower, to take measures to stabilize the grid. This could involve activating more expensive backup power sources, such as gas-fired power plants, or implementing demand-side management programs. The cost of operating these backup systems for an extended period could amount to millions of dollars. Additionally, the grid instability caused by the outage could potentially lead to other indirect costs across the economy.

8. Conclusions

Among the three wind turbine types, onshore ones are the most resilient to missile and aviation attacks due to their robust towers, with the nacelle being the main vulnerability, which can be protected by metal mesh grids.

Offshore fixed-bottom turbines share similar construction but are harder to repair as they require specialised vessels, which are also targets. Submarine cables are vulnerable, so they should be buried, kept confidential, and installed by trusted contractors.

Floating offshore turbines have reinforced towers but are prone to attacks on their floating platforms, mooring systems, and dynamic cables. To enhance their survivability, platforms should have smaller waterlines with more compartments, steel mooring chains, additional mooring lines, and greater spacing between units.

Cyberattacks have dealt profuse damage to the energy industry in the last decade. They are particularly dangerous as they can be used without declaring a war or sending troops. Offshore wind farms are particularly susceptible to Denial-of-Service attacks due to the difficulty of access for repairs. Mitigation measures are currently only being developed, as holes in the defences can come from the smallest component of the system.

Some of the above risks can be mitigated, incurring additional expenses, which amount to a maximum of 6.71% of total farm cost for land-based turbines, 8.19% for fixed-bottom offshore, and 12.72% for floating wind turbines. This makes land-based turbines the most easily protected, while both types of offshore turbines have risks that might be impossible to mitigate.

Author Contributions

Conceptualization, G.I. and Y.P.; investigation, G.I.; methodology, G.I. and Y.P.; resources, Y.P.; software, G.I.; visualization, G.I.; writing—original draft, G.I.; writing—review and editing, Y.P. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable. Study not involving humans.

Data Availability Statement

All data is contained within the article.

Acknowledgments

The authors thank Prof. Kai-Tung Ma, National Taiwan University for providing high-quality wind turbine renderings.

Conflicts of Interest

The authors disclosed no conflict of interest.

References

[1] Maliarchuk, T., Danyk, Y. Briggs, C., 2019. Hybrid warfare and cyber effects in energy infrastructure. Connections. 18(1/2), 93 –110. DOI: https://doi.org/10.11610/Connections.18.1-2.06

[2] Farrell, A.E., Zerriffi, H., Dowlatabadi, H., 2004. Energy infrastructure and security. Annual Review of Environment and Resources. 29(1), 421–469. DOI: https://doi.org/10.1146/annurev.energy.29.062403.102238

[3] Kosse, I., 2023. Rebuilding Ukraine's infrastructure after the war. Policy Notes and Reports 72, 02 November 2023.

[4] Binetti, M.N., 2023. Rebuilding energy infrastructures and the manufacturing sector in post-conflict countries. Energy Policy. 172, 113298. DOI: https://doi.org/10.1016/j.enpol.2022.113298

[5] Stengrundet, A., 2023. From Headwinds to Tailwinds? A Comparison of Norwegian Households' Willingness to Pay for Wind Power Before and After the War Outbreak in Ukraine [Master Thesis]. Norwegian University of Life Sciences: Akershus, Norway.

[6] Stehly, T., Duffy, P., Mulas Hernando, D., 2024. Cost of Wind Energy Review: 2024 Edition. National Renewable Energy Laboratory (NREL): Golden, CO, USA.

[7] Sanderson, C., 2024. 'Standing tall': Ukraine's wind turbines are proving a key tactical advantage, says industry chief. Available from: https://www.rechargenews.com/wind/standing-tall-ukraines-wind-turbines-are-proving-a-key-tactical-advantage-says-industry-chief/2-1-1657698 (cited 3 March 2025).

[8] Ivanov, G., 2024. Ukraine – Taiwan offshore wind joint venture. Promising cooperation for achieving energy independence. International Journal of Business. 29(3), 005.

[9] Lilas, T., Dagkinis, I.K., Nikitakos, N., et al., 2011. Green offshore structures, promising viable utilization of shipyard facilities. Journal of Shipping and Ocean Engineering. 1, 1–7.

[10] BVG Associates, Guide to a Floating Offshore Wind Farm, 2023. The crown estate and crown estate Scotland: Offshore renewable energy catapult. Available from: https://guidetofloatingoffshorewind.com/wp-content/uploads/2023/06/BVGA-16444-Floating-Guide-r1.pdf (cited 01 April 2025).

[11] Sørensen, J.D., 2006. Structural Reliability Aspects in Design of Wind Turbines. Proceedings of The Rackwitz Symposium; November 24, 2006; Munich, Germany. pp. 1–31. Available from: https://www.rackwitz-symposium.ethz.ch/presentations/04_Rackwitz-symp-24nov2006-jds.pdf (cited 01 April 2025).

[12] Zou, T., Niu, X., Ji, X., et al., 2022. The impact of initial imperfections on the fatigue assessment of tower flange connections in floating wind turbines: A review. Frontiers in Marine Science. 9, 1–16. DOI: https://doi.org/10.3389/fmars.2022.1063120

[13] Chou, J.-S., Ou, Y.-C., Lin, K.-Y., 2019. Collapse mechanism and risk management of wind turbine tower in strong wind. Journal of Wind Engineering and Industrial Aerodynamics. 193, 103962. DOI: https://doi.org/10.1016/j.jweia.2019.103962

[14] Uadiale, S., Urbán, E., Carvel, R., et al., 2014. Overview of problems and solutions in fire protection engineering of wind turbines. Fire Safety Science. 11, 983–995.

[15] Yu, H.-Z., 2022. Water Mist Protection of Wind Turbine Nacelles. Proceedings of The 2022 International Water Mist Conference; November 9–10, 2022; Madrid, Spain. pp. 1–20. Available from: https://iwma.net/fileadmin/user_upload/IWMC_2022/Yu_FMGlobal_IWMC2022.pdf (cited 01 April 2025).

[16] Tepper, J.; Murillo, R.; Roy, C.; et al., 2011. Dry-Type Transformers for the 72.5 kV Voltage Class. Proceedings of The 21st International Conference on Electricity Distribution; June 6–9, 2011; Frankfurt, Germany. pp. 68–98.

[17] Garidis, G., Offshore Wind Power Modeling and Forecasting with Very High-Resolution Weather Forecasts [Master's thesis]. University of Copenhagen: Copenhagen, Denmark.

[18] Kulsinskas, A., Durdevic, P., Ortiz-Arroyo, D. 2021. Internal wind turbine blade inspections using UAVs: Analysis and design issues. Energies. 14(2), 294.

[19] Rajamohan, S., Vinod, A., Aditya, M., et al., 2022. Approaches in performance and structural analysis of wind turbines – A review. Sustainable Energy Technologies and Assessments. 53, 102570. DOI: https://doi.org/10.1016/j.seta.2022.102570

[20] Mitchell, D., Blanche, J., Harper, S., et al., 2022. A review: Challenges and opportunities for artificial intelligence and robotics in the offshore wind sector. Energy and AI. 8, 100146. DOI: https://doi.org/10.1016/j.egyai.2022.100146

[21] Ivanov, G., Ma, K.-T., 2024. Floater assembly and turbine integration strategy for floating offshore wind energy: Considerations and recommendations. Wind. 4(4), 376–394.

[22] Maloney, D., 2024. 80% of insurance claims in offshore wind are related to subsea cable failures – How can the industry manage these risks?. Available from: https://www.dnv.com/article/80-percent-of-insurance-claims-in-offshore-wind-are-related-to-subsea-cable-failures-how-can-the-

industry-manage-these-risks/ (cited 30 March 2024).

[23] Warnock, J., McMillan, D., Pilgrim, J., et al., 2019. Failure rates of offshore wind transmission systems. Energies. 12(14), 2682.

[24] Duggal, R.H., 2020. Guyana submarine cable suffers an anchor damage. Available from: https://www.4coffshore.com/news/guyana-submarine-cable-suffers-an-anchor-damage-nid20640.html (cited 01 February 2025).

[25] Braw, E., 2023. Chinese-made wind farms could become a new sabotage risk. Available from: https://www.ft.com/content/eb1bb373-07a8-48f8-b5e6-aa3c9ed98e64 (cited 02 February 2025).

[26] Hale, E., 2025. As undersea cables break off Europe and Taiwan, proving sabotage is tough. Available from: https://www.aljazeera.com/news/2025/3/10/as-undersea-cables-break-down-proving-difficult-task (cited 10 March 2025).

[27] Kirsten Tallow, D. , 2025. Exclusive—Chinese patents reveal aim to cut undersea cables. Available from: https://www.newsweek.com/china-conflict-undersea-cables-cutting-internet-data-subsea-marine-baltic-taiwan-2012396 (cited 10 January 2025).

[28] Agency for the Cooperation of Energy Regulators, 2015. Report on Unit Investment Cost Indicators and Corresponding Reference Values for Electricity and Gas Infrastructure. European Union. Available from: https://www.acer.europa.eu/sites/default/files/documents/Official_documents/Publications/UIC_Electricity_History/UIC%20Report%20%20-%20Electricity%20infrastructure.pdf (cited 1 April 2025).

[29] Dunkirk Wind Park, 2019. A 600 MW wind project off the coast of Dunkirk. 2019. Available from: https://parc-eolien-en-mer-de-dunkerque.fr/project-en/ (cited 11 March 2025).

[30] Japan International Cooperation Agency, 1982. Master Plan Report of Electric Distribution System in Bangkok. Report number (JICA Library): 1050027[0], August 1982. Available from: https://openjicareport.jica.go.jp/pdf/11253325_11.pdf (cited 02 April 2025).

[31] Hsu, I.-J.; Ivanov, G.; Ma, K.-T.; et al., 2022. Optimization of Semi-Submersible Hull Design for Floating Offshore Wind Turbines. Proceedings of The 41st International Conference on Offshore Mechanics and Arctic Engineering (OMAE 2022); June 5–10, 2022; Hamburg, Germany. pp. 1–12. DOI: https://doi.org/10.1115/OMAE2022-86751

[32] Ivanov, G., Hsu, I.-J., Ma, K.-T., 2023. Design considerations on semi-submersible columns, bracings and pontoons for floating wind. Journal of Marine Science and Engineering. 11(9), 1663. DOI: https://doi.org/10.3390/jmse11091663

[33] Xu, K., Larsen, K., Shao, Y., et al., 2021. Design and comparative analysis of alternative mooring systems for floating wind turbines in shallow water with emphasis on ultimate limit state design. Ocean Engineering. 219, 108377. DOI: https://doi.org/10.1016/j.oceaneng.2020.108377

[34] Ma, K.-T., Huang, W.-Y., Wu, K.-Y., et al., 2025. Wind farm design with 15 MW floating offshore wind turbines in typhoon regions. Journal of Marine Science and Engineering. 13(4), 687. DOI: https://doi.org/10.3390/jmse13040687

[35] Lin, Y.-H., Huang, Y.-R., 2022. Drift simulation of a floating offshore wind turbine with broken mooring lines in a dynamic sea condition. Ocean Engineering. 266, 112729. DOI: https://doi.org/10.1016/j.oceaneng.2022.112729

[36] Ivanov, G.; Wu, Y.; Chen, D.; et al., 2024. Optimal Mooring Pattern for a Semi-Submersible FOWT in a Typhoon Environment. Proceedings of The 43rd International Conference on Ocean, Offshore and Arctic Engineering (OMAE2024); June 9–14, 2024; Singapore. pp. 1–12.

[37] Det Norske Veritas, 2025. Energy Cyber Priority 2025: Addressing Evolving Risks, Enabling Transformation. Available from: https://www.dnv.com/cyber/insights/publications/energy-cyber-priority-2025/ (cited 12 April 2025).

[38] Styczynski, J., Beach-Westmoreland, N., 2019. When the lights went out: A comprehensive review of the 2015 attacks On Ukrainian critical infrastructure. Available from: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf (cited 12 April 2025).

[39] Pollard, M., 2024. A case study of russian cyber-attacks on the Ukrainian power grid: Implications and best practices for the United States. Pepperdine Policy Review. 16(1), 1.

[40] Salazar, L.; Castro, S.R.; Lozano, J.; et al., 2024. A Tale of Two Industroyers: It was the Season of Darkness. Proceedings of The 2024 IEEE Symposium on Security and Privacy (SP); May 19–23, 2024. San Francisco, CA, USA. pp. 312–330.

[41] Proska, K., Wolfram, J., Wilson, J., et al., 2023. Sandworm disrupts power in Ukraine using a novel attack against operational technology. Available from: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/ (cited 02 April 2025).

[42] Mura, A., 2022 An analysis of the cyberattack against ViaSat of February 2022. Available from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwijhsLqiY6NAxVWh1YBHXubGGYQFnoECBkQAQ&url=https%3A%2F%2Fcentri.unibo.it%2Fcomputational-social-science%2Fit%2Fcosa-facciamo%2Four-students-papers%2Fmura_cs-cw2024_final.pdf%2F%40%40download%2Ffile%2FMura_CS%26CW2024_FINAL.pdf&usg=AOvVaw1aEW3vzuAHpJGqC9YvOgmE&opi=89978449 (cited 02 April 2025).

[43] Quiquet, F., 2025. Enhancing threat understanding: Modeling the viasat cyber attack with MITRE CTID's attack flow builder. Available from: https://www.spacesecurity.info/en/how-i-modeled-the-viasat-cyber-attack-to-leverage-attack-flow-builder-from-mitre-for-enhanced-threat-understanding/ (cited 02 April 2025).

[44] Boschetti, N.; Gordon, N.G.; Falco, G., 2022. Space Cybersecurity Lessons Learned from the Viasat Cyberattack. Proceedings of The ASCEND 2022; October 24–26, 2022; Las Vegas, NV, USA. pp. 4380.

[45] Gabbatt, A., 2021. How the Colonial Pipeline hack is part of a growing ransomware trend in the US. Available from: https://www.theguardian.com/technology/2021/may/13/colonial-pipeline-ransomware-attack-cyber-crime (cited 14 April 2025).

[46] Mohammed, A.S., Reinecke, P., Burnap, P., et al., 2022. Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (ICPS) perspective. ACM Transactions on Cyber-Physical Systems (TCPS). 6(3), 1–27

[47] Chen, J.; Du, H.; Yan, J.; et al., 2023. A Data Integrity Attack Targeting VSC-HVDC-Connected Offshore Wind Farms. Proceedings of The 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). 3 November 2023; Glasgow, UK. pp. 1–6. DOI: https://doi.org/10.1109/SmartGridComm57358.2023.10333872

[48] Topallaj, K., McKerrell, C., Ramanathan, S., et al., 2025. Impact assessment of cyberattacks in inverter-based microgrids. DOI: https://doi.org/10.48550/arXiv.2504.05592

[49] Presekal, A., Rajkumar, V.S., Ştefanov, A., et al., 2025. Cyberattacks on power systems. In: Parizad, A., Baghaee, H.R., Rahman, S. (eds.). Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions. Publisher: Wiley. pp. 365–403.

[50] Dolezilek, D.; Gammel, D.; Fernandes, W., 2020. Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems. Proceedings of The 15th International Conference on Developments in Power System Protection (DPSP 2020); (March 9-12, 2020); Liverpool, United Kingdom.

[51] Idima, S., Nwaga, P., Evah, P., 2025. Comprehensive analysis of SCADA system data for intrusion detection using machine learning. Global Journal of Engineering and Technology Advances. 22, 064–089. DOI: https://doi.org/10.30574/gjeta.2025.22.2.0027

[52] Dao, P.B., Barszcz, T., Staszewski, W.J., 2024. Anomaly detection of wind turbines based on stationarity analysis of SCADA data. Renewable Energy. 232, 121076

[53] Farrar, N., Ali, M.H., 2024. Cyber-resilient converter control system for doubly fed induction generator-based wind turbine generators. Electronics. 13(3), 492.

[54] Baezner, M., Robin, P., 2017. Stuxnet. ETH Zurich. Available from: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/200661/Cyber-Reports-2017-04.pdf (cited 14 April 2025).

[55] Raggi, M., Scenarelli, S., 2020. Rising tide: Chasing the currents of espionage in the South China sea. Available from: https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea (cited 14 April 2025).

[56] Wang, L., Industrial users' power rates to rise 12.5% on average. Available from: https://www.taipeitimes.com/News/front/archives/2024/10/01/2003824615 (cited 14 April 2025).

[57] Morris, G., 2023. Replacing offshore wind turbines costs millions. What north american operators can learn from Europe's loss lessons. Available from: https://riskandinsurance.com/replacing-offshore-wind-turbines-costs-millions-what-north-american-operators-can-learn-from-europes-loss-lessons/ (cited 14 April 2025).