

CeSI | CENTRO STUDI INTERNAZIONALI

FROM ENERGY TRANSITION TO SECURITY CHALLENGE:
CHINESE WIND TURBINES IN EUROPE

November 2026

CeSI | CENTRO STUDI INTERNAZIONALI

FROM ENERGY TRANSITION TO SECURITY CHALLENGES:

CHINESE WIND TURBINES IN EUROPE

November 2026

Explore all our **programmes**

- Africa
- Americas
- Asia and Pacific
- Defence and Security
- Europe
- Geoeconomics
- Middle East and North Africa
- Russia and Caucasus
- Terrorism and Radicalisation
- Conflict Prevention
- Xiáng

INDEX

SUMMARY 1

FINDINGS AND POLICY RECOMMENDATIONS 4

INTRODUCTION AND ANALYSIS OF THE STRATEGIC AND POLITICAL CONTEXT 7

SECTION I: ASSESSMENT OF CURRENT AND PROJECTED PRESENCE OF CHINESE ACTORS IN THE EU WIND SECTOR 11

1. Mapping Chinese presence in Europe 12
2. Industrial and commercial presence of Chinese companies 13
3. Vulnerability analysis and the risk of "solarization" 15
4. Projective conclusion 17

SECTION II: TECHNICAL ANALYSIS OF ATTACK PATHS AND SECURITY VULNERABILITIES LINKED TO CHINESE WIND TURBINES IN EUROPE 18

1. Technical architecture and high-impact attack paths of modern wind turbines 19
2. Chinese exposure in critical components and weaponization potential 22
3. Structured security risk assessment 24
4. Plausible scenarios 26

SECTION III: CHINESE COMPANIES IN EUROPE AND RESTRICTIONS ON EU COMPANIES IN THE CHINESE MARKET 29

1. Chinese presence in the European wind ecosystem 29
2. Links with Chinese security apparatuses: regulatory framework and corporate profiles 31
3. Chinese domestic security practices, market asymmetry and the relevance of the Cybersecurity Act 2 33

SUMMARY

Europe's necessary green ambitions are driving growth in clean energy. Demand for wind installations is rising, and yet this market is increasingly shaped by one actor: China, whose state subsidies are distorting competition. Chinese original equipment manufacturers (OEMs) offer industrial scale, greater capacity, and turbines at prices that European manufacturers struggle to match, deprived of similar levels of government intervention. Yet as energy assets – solar and nuclear, as well as wind – become more digitalized and more closely integrated into electricity networks, security is becoming a critical issue. The identity and technical position of suppliers are now factors driving a broader energy infrastructure challenge.

In fact, Chinese competition in the European wind ecosystem takes several forms and creates different dependencies. Component suppliers affect industrial resilience and supply chain concentration. Investors and operators raise questions about ownership, management and access. Grid investments impact network governance and sensitive system information.

However, OEMs occupy a specific and critical position. Modern wind turbines are not just mechanical devices: they are connected cyber physical assets whose functions depend on interaction between mechanical systems, electrical conversion, control logic, communications networks and data flows.

Given this sophistication, OEMs maintain significant lifelong influence over the turbine as an integrated asset. Dependency on an OEM continues beyond procurement and installation, and throughout the turbine's lifetime, via maintenance, diagnostics, software updates and routine system management, proprietary software, firmware, embedded controllers, diagnostics, updates, data interfaces, and remote access channels. The OEM maintains access, influence and control.

In this context, European operators working with Chinese OEMs may seek to restrict external access, reduce reliance on the OEM's proprietary environment, or insist on local manufacturing, monitoring centers, or Operation and Maintenance. However, such measures merely create an illusion of control and oversight, and a false sense of security. In reality, OEM dependency persists, ultimately allowing Chinese manufacturers control over wind turbines installed in Europe.

When it comes to potentially exercising that influence and control, the report identifies two connected threat vectors. Technological weaponization can occur through control system vulnerabilities. Wind farms rely on SCADA (Supervisory Control and Data Acquisition) systems, Operational Technology networks, and remote access functions. Interference could produce loss of visibility, manipulated data monitoring/transmission, unauthorized commands, altered parameters, or delayed responses. Wind farms can also gather infrastructure intelligence, identify faults, and collect grid-related data to support grid resilience.

In the current political and geostrategic context, these are plausible scenarios: Chinese companies are legally obliged to support, assist and cooperate with state intelligence work, and in cases provide technical assistance to public security and state security services[1]. OEMs necessarily collect data and control access; but when an OEM holds this power it also presents a clear, identifiable risk to Europe's energy infrastructure, raising the possibility of compromise, sabotage and weaponization of individual wind turbine assets, endangering general grid stability.

Through the Cyber Resilience Act (CRA), Europe has established horizontal cybersecurity requirements for products with digital elements. However, the proposed revision of the Cybersecurity Act (CSA2) offers a vehicle for a risk-based approach to high-risk suppliers and ICT supply chains, including non-technical factors. For wind, this should mean addressing actors that retain significant influence over connected assets throughout their operational life.

Our recommendation is to apply CSA2 to high-risk direct suppliers of assets that connect to critical infrastructure (including turbines). In practice, this means suppliers with whom an asset owner or operator has a direct contractual supply relationship and whose risk profile has been established through the relevant assessment framework (based on controlling ownership rather than location of production or headquarters). Given OEMs' persistent capacity to control - affecting software, firmware, diagnostics, access rights, data interfaces and operational functions - they should be covered by this definition. Introducing restrictions covering only direct suppliers would unburden companies of bureaucratic and disproportionate checks deep into

[1] National People's Congress Standing Committee, *National Intelligence Law of the P.R.C.* (2017), China Law Translate (English translation), https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

supply chains that could weaken the competitiveness of the European wind industry without delivering equivalent gains in cybersecurity.

In this broader context, sector-specific implementation is essential. Wind infrastructure is distinctive, with long asset lifecycles, remote connectivity, proprietary control systems and close integration with the electricity grid. In conjunction with the CRA, targeted measures and sandboxed solutions under CSA2 can develop into workable requirements that strengthen energy security, economic resilience and Europe's ability to retain effective control over critical energy assets, helping the EU to fulfil its green ambitions.

FINDINGS AND POLICY RECOMMENDATIONS

The proposed revision of the Cybersecurity Act (CSA2) provides the European Union with a relevant vehicle to address some of the vulnerabilities identified in this report. The central policy challenge is to ensure that the regulatory response remains proportionate, operationally workable, and focused on the actors that may retain meaningful influence over connected wind energy assets.

Key findings

1. Wind turbines should be assessed as integrated cyber-physical assets. The main security concern does not arise from the origin of individual components. It concerns the capacity to affect the functionality of the turbines throughout their lifecycles through software, firmware, diagnostics, update pathways, data interfaces, access rights and operational functions.
2. The OEM occupies the key position in a risk assessment. A Chinese OEM retains influence over the asset after installation because proprietary architectures and digital interfaces remain essential to its functioning. Attempted mitigations such as assembly in Europe, local monitoring centers or European Operation and Maintenance, may provide some autonomy but ultimately present an illusion of access, influence, and control. Ultimate effective control would remain with the Chinese OEM, which has legal obligations to provide support to Chinese state security services upon request.
3. The security risks are broader than industrial dependence, such as supply-chain concentration and market distortion. However, the most significant infrastructure risk is due to an OEM's long-term and necessary access to connected assets. This gives an OEM influence over the turbine's availability, visibility, or behavior, including turbine software, control logic, update mechanisms or plant-level operational functions. Putting such access, influence and control in the hands of a high-risk OEM creates exposure to economic coercion, technological interference and data exploitation.

4. Exposure extends beyond the turbine, leading to wider exposure to the electricity grid and potentially devastating consequences. Such exposure should not be understood as requiring direct access to TSO or DSO systems. Material effects may arise through the turbines themselves, given the OEM's access, influence and control, which may affect system stability, operational predictability and coordinated response capabilities. These risks can occur even in the absence of direct access to grid-operator infrastructure.
5. Control over a turbine remains the most significant exposure from high-risk suppliers. A component-by-component approach under CSA2 risks being disproportionate. Deep investigations across lengthy supply chains could impose substantial administrative burdens and weaken the competitiveness of the European wind industry without delivering equivalent gains in security or addressing the most relevant operational risks.

Main policy recommendation: focus CSA2 on direct-source high-risk suppliers

The application of the relevant ICT supply-chain restrictions and obligations under CSA2 should focus on direct-source high-risk suppliers, whose risk profile has been established through the assessment framework provided by the regulations.

In the wind sector, this approach would mean scrutiny of OEMs, whose role in the integrated asset (the turbines) creates a persistent capacity to access, influence and control via software, firmware updates, diagnostics, data interfaces, access rights or operational functions. Where the assessment identifies an OEM as a high-risk supplier, the regulator should be capable of restricting such assets from being supplied. This approach would serve the central purpose of CSA2 but avoid disproportionate obligations throughout the entire supply chain and the treatment of upstream input as an autonomous source of exposure merely because of its country of origin.

Sector-specific implementation

CSA2 should also recognize the distinctive characteristics of different sectors. Wind, especially, is characterized by long asset lifecycles, remote connectivity, proprietary control systems, and close integration with the electricity grid.

Sector-specific measures and sandboxed solutions could translate the direct-source approach into workable requirements for wind projects. Their purpose would be to protect European energy infrastructure without imposing unnecessary burdens on firms or pursuing industrial protectionism. A proportionate OEM-focused framework would support energy security, economic resilience, and the Union's capacity to retain effective control over the assets that underpin its decarbonization strategy.

INTRODUCTION AND ANALYSIS OF THE STRATEGIC AND POLITICAL CONTEXT

Key Takeaways

- *Wind power has become a long-term structural pillar of Europe's energy system. At the same time, Chinese state-subsidized industrial growth is creating a price differential that places sustained pressure on European manufacturers, specialized skills and research capacity.*
- *Wind turbines are sophisticated connected cyber-physical assets. The original equipment manufacturer (OEM) and the proprietary architecture can shape the operator's degree of autonomy, making the role of the OEM a more significant factor than involvement of a European operator or having a European manufacturing location.*
- *Oversight should avoid a highly granular, component-centered approach. Such an approach would miss the main source of exposure, related to factors such as control, remote access, long-term or lifetime dependences, and access to operational data.*

Wind expansion as part of Europe's decarbonization strategy

Europe's decarbonization strategy has transformed wind power from a fast-growing renewable segment into a long-term structural pillar of its energy system. Wind project investments being made today will commonly operate for 25 to 35 years. This brings new challenges, as supplier relationships, software dependencies and threat environments may change during that time. The central question is whether European operators can preserve oversight and continuity of service under adverse conditions.

This question is particularly pertinent because Europe's wind expansion takes place within a global market increasingly shaped by state-subsidized Chinese industrial growth. In 2025, China accounted for approximately 70% of new global wind installations and had a cumulative installed base exceeding 630 GW[2]. The majority of this growth came in China, a domestic market of exceptional size that is effectively closed to external suppliers. Domestic growth is supplemented by external expansion, aided by state subsidies that

[2] Karlien Sambell et al., *The EU's China Challenge: Rethinking Offshore Wind and Electrolysis Strategy*, HCSS - The Hague Center for Strategic Studies, TNO Public / TNO 2024 R10732 (May 2024), https://hcss.nl/report/the-eus-china-challenge-rethinking-offshore-wind-and-electrolysis-strategy/.

affect competitive conditions. When looking at capital expenditure (CAPEX) alone, Chinese turbines are estimated to be 30–40% cheaper than Western alternatives on average: this differential may place sustained pressure on European manufacturers, their workforce and their research capacity.[3]

Recent investment initiatives have reinforced this shift. In 2024, MingYang signed an agreement to establish a manufacturing plant in Italy, with an estimated investment of €500 million.[4] In 2025, the company also announced plans for a £1.5 billion facility in Scotland, subsequently blocked by the UK government.[5] These cases signal a transition from export-led penetration towards a more embedded presence in European manufacturing.

However, while local production may reduce logistical constraints, it does not by itself reduce the risk of unwanted nation state interference over the turbine software, update pathways, diagnostics and operational interfaces. This is due to Chinese controlling ownership and the obligation under China's National Intelligence Law for organizations and citizens to support, assist and cooperate with state intelligence work.

Mitigating risks to the operation of turbines, sophisticated connected cyber-physical assets

A modern wind turbine is a connected cyber-physical asset. Its operation depends on software, sensors, control systems, remote monitoring platforms and data flows. Exposure extends beyond initial procurement, persisting throughout installation, maintenance, diagnostics, updates and system management. In this context, the original equipment manufacturer, or OEM, has a central role because its proprietary architecture can shape the operator's degree of autonomy over the complete asset.[6]

[3] Andrea Scassola, "Chinese OEMs in the European Wind Market: Cost Advantage Meets Credibility Gaps," *Rystad Energy*, April 24, 2025, https://www.rystadenergy.com/insights/chinese-oems-in-the-european-wind-market-cost-advantage-meets-credibility-gaps

[4] "China's MingYang Signs Italy Wind Turbine Plant Deal," *Reuters*, August 8, 2024, https://www.reuters.com/business/energy/chinas-mingyang-signs-italy-wind-turbine-plant-deal-2024-08-08/.

[5] "Chinese firm's Highland port plans blocked by UK government," *BBC News*, March 25, 2026 https://www.bbc.com/news/articles/c995xjxk97mo

[6] Michal Meidan and Anders Hove, *Chinese Participation in Europe's Offshore Wind Sector: The Good, the Bad and the Unknown*, Oxford Institute for Energy, OIES Paper: CE 17, (OIES, 2025),

The most relevant areas of exposure are:

- Software updates, firmware and remote diagnostics, which can create recurring access points;
- Operational data, which could provide information on plant performance and grid behavior;
- Remote-control functions, whose misuse could affect generation availability or operational continuity.

The involvement of a European operator can mitigate these risks when it strengthens oversight, limits external access and preserves continuity of service. However, in practice this risk mitigation is dependent on the level of autonomy that the operator can exercise in relation to the OEM. Any risk assessment should therefore consider whether the operator can manage routine functions, verify access arrangements and maintain the asset under adverse conditions, without excessive dependence on proprietary tools or services.

The assignment of operational responsibilities to a European actor is relevant, but it does not automatically remove exposure where essential functions remain tied to the manufacturer's technological environment. The physical location of production is not a reliable indicator of risk: a turbine *assembled inside Europe* may still operate within a digital and operational environment that is *controlled outside Europe*. Likewise, the presence of internationally sourced components is not in itself a security concern; the decisive issue is the structure of control over the integrated turbine.

Risk-based oversight focused on operational control

The policy implication is that oversight should avoid a highly granular approach centered on individual components. Such an approach would be burdensome and could miss the main source of exposure. A more effective assessment should concentrate on the functions that determine operational control and on the relationship between the OEM and the operator.

Three questions are especially relevant:

https://www.oxfordenergy.org/wpcms/wp-content/uploads/2025/10/CE17-Chinese-participation-in-Europes-offshore-wind-sector.pdf.

- Who controls remote access, software updates, firmware and diagnostic pathways?
- What are the risks related to long-term or lifetime dependency on physical spare parts and digital updates from a Chinese vendor, even if the turbine is managed by a European operator?
- Who can access operational data and the interfaces through which those data are managed?

These questions apply to both onshore and offshore wind installations: offshore concentrates significant generating capacity in assets with longer development and maintenance timelines;[7] meanwhile, onshore remains relevant because it forms a substantial part of Europe's wind fleet and is integrated into the same broader energy system.

Europe's wind strategy therefore requires a risk-differentiated framework focused on remote access, operational governance and lifecycle dependency. The purpose is not to attribute hostile intent based on nationality or component origin. It is to identify cases in which an OEM's technological position may create persistent exposure within critical energy infrastructure. As wind power becomes more important for Europe's energy system, this distinction is essential so that faster deployment remains compatible with resilience and effective control.

[7] Sambell et al., *The EU's China Challenge.*

SECTION I: ASSESSMENT OF CURRENT AND PROJECTED PRESENCE OF CHINESE ACTORS IN THE EU WIND SECTOR

Key Takeaways

- *Supported by substantial state subsidies, Chinese OEMs are building industrial scale and sustained price pressure that may weaken Europe's manufacturing capacity, creating both the potential for "solarization" and a reliance on connected turbines, generating security risks.*
- *Chinese participation in Europe includes OEMs, component suppliers, asset owners, operators and grid-related investments, but these categories create different forms of exposure and require distinct assessments.*
- *Local manufacturing or operations do not remove dependency on OEMs' proprietary software, embedded controllers, diagnostic tools, updates, and operational interfaces, and therefore cannot eliminate security risks.*

The global wind industry is entering a phase in which Chinese OEMs are major competitors – aided by a closed domestic market and state subsidies that enhance their competitive position internationally. In 2025, the three leading turbine manufacturers worldwide were Goldwind, Envision and Windey[8]. This industrial position reflects the scale of the Chinese domestic market, large manufacturing capacity and public support measures (including subsidies) that affect the competitive balance with European firms.

As a result, Chinese OEMs can offer turbines at prices estimated to be 30–40% below Western alternatives (in terms of capital expenditure9)[10], but in terms of levelized cost of electricity (LCOE), the overall costs of turbines from Chinese

[8] "Chinese OEMs Sweep the Global Wind Podium for the First Time. Goldwind Leads with 20 GW Installed, Followed by Envision and MingYang," *Wood Mackenzie,* March 14, 2025, https://www.woodmac.com/press-releases/2024-press-releases/chinese-oems-sweep-the-global-wind-podium-for-the-first-time/.

[10] Andrea Scassola, "Chinese OEMs in the European Wind Market: Cost Advantage Meets Credibility Gaps," *Rystad Energy*, April 24, 2025, https://www.rystadenergy.com/insights/chinese-oems-in-the-european-wind-market-cost-advantage-meets-credibility-gaps

OEMs can be higher, factoring in higher financing costs, transportation and warranty costs, and - crucially - increased risks of state-sponsored interference and attacks.

The relevance for Europe is not simply one of market share. It is industrial policy- *and* security policy-related: it is about aggressive, state-subsidized price competition that leads to dependence on non-European proprietary software, firmware, diagnostics, updates and remote access.

1. Mapping Chinese presence in Europe

Chinese presence in the European wind sector has moved beyond indirect participation in the supply chain. It now includes potential manufacturing facilities, pipeline projects, OEM partnerships, component suppliers, renewable asset ownership and, in the broader energy system, participation in grid-related infrastructure. These channels differ in nature but point to the same policy challenge: Chinese operational influence over the turbine as an integrated asset.

The MingYang investments highlight that Chinese OEMs may seek a more permanent position within Europe's industrial base. Although local manufacturing may reduce logistical barriers and create employment benefits, the central security issue remains: a turbine assembled in Europe will still depend on a foreign OEM for embedded controllers, firmware, diagnostic tools, software updates and proprietary operational interfaces.

Commercial penetration also proceeds through long-term project arrangements. The Octopus Energy–MingYang partnership in the United Kingdom, although outside EU territory, illustrates the limits of a simple division between Chinese hardware and European software.[11] Retaining a supervisory software layer does not necessarily give the operator control over the embedded real-time controllers that govern core functions of a turbine: pitch control, yaw alignment, braking logic, generator torque, converter behavior and safety routines. These functions are part of the OEM's integrated turbine

[11] Michal Meidan and Anders Hove, "Experts: Will Chinese Wind Power Help or Hinder Europe's Climate Goals? - Carbon Brief," *Carbon Brief - Clear on Climate*, January 30, 2026, https://www.carbonbrief.org/experts-will-chinese-wind-power-help-or-hinder-europes-climate-goals/.

architecture. They cannot be replaced without major redesign, certification, and safety implications. The relevant question is therefore whether the operator *supervises* the asset, or whether it can effectively *control and sustain it* under adverse conditions.

For example, the Luxcara case in Germany shows how this distinction is already affecting procurement decisions. The initial award to MingYang for the 300 MW Waterkant project was reversed in favor of Siemens Gamesa after national security concerns were raised.[12] The episode does not prove hostile intent by a specific supplier. It does show that the security profile of a wind project is increasingly assessed through the integrity of the OEM's control architecture and the degree of operational autonomy retained by the European operator.

Beyond the turbine, Chinese participation in grid infrastructure adds a separate layer of exposure. Entities linked to the People's Republic of China hold or have sought stakes in European energy networks, including SGCC's 25% stake in REN in Portugal, as well as links to Terna through CDP Reti, Creos in Luxembourg, Enemalta in Malta and IPTO/ADMIE in Greece.[13] This issue should remain analytically distinct from turbine OEM risk. TSO participation concerns network governance, system information, and investment influence. OEM risk concerns the operational and digital control of the turbine. However, together they show that Chinese presence may affect several layers of Europe's electricity system, from generation assets to network infrastructure.

2. Industrial and commercial presence of Chinese companies

The main Chinese OEMs have already established, or attempted to establish, a stronger position in Europe. **MingYang** combines industrial localisation with project-level ambition, as shown by the Italian plant agreement, the blocked Scottish facility and the Waterkant procurement episode. **Envision** has research and development centers in Germany and Denmark and has

[12] Ibid

[13] Caspar Hobhouse, "The Dragon in the Grid: Limiting China's Influence in Europe's Energy System," *European Union Institute for Security Studies*, (EUSS, January 2026), https://www.iss.europa.eu/publications/briefs/dragon-grid-limiting-chinas-influence-europes-energy-system.

pursued operational partnerships with European actors.[14] On this matter, its 2025 agreement with Global Energy Services in Spain covers development, construction, storage and Operation and Maintenance (O&M) activities across Spain and the rest of Europe.[15]

This type of cooperation should be assessed carefully. European O&M participation can mitigate risk if it increases access control, operational visibility and continuity of service. However, it should not be treated as a catch-all when a Chinese OEM still controls core turbine architecture, firmware, proprietary diagnostic tools or update mechanisms. The biggest risk is linked to the OEM's technical position in the asset. European O&M participation may reduce that exposure, but it does not remove it entirely.

Goldwind represents a different form of relevance. Its European presence is less visible in individual projects, yet it has become a central case for EU scrutiny under the Foreign Subsidies Regulation. In 2026, the European Commission opened an in-depth investigation into whether Goldwind benefited from foreign subsidies, including grants, preferential tax measures and concessional loans, that could distort the internal market for wind turbines and related services.[16] The case is important because it links the OEM question to the level-playing-field problem. Subsidized market entry can weaken European industrial capacity and accelerate dependence on suppliers whose role may later extend into software-dependent assets. Goldwind's controlling stake in Vensys Energy also shows that Chinese OEM presence may occur through European subsidiaries, not only through direct exports.

Chinese suppliers are also present in less visible parts of the wind value chain. **Dajin Heavy Industry** is involved in the Gennaker offshore project in the Baltic Sea through the supply of transition pieces for large-scale turbines.[17] It has also signed an agreement to establish an offshore foundations facility at the

[14] Envision Energy, "Global Locations," (2021), https://www.envision-energy.in/global#.
[15] Ibid
[16] European Commission, "Commission Opens In-Depth Foreign Subsidies Investigation into Goldwind's Activities in the EU Wind Sector," European Commission Press Corner, February 3, 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_265.
[17] Edward Peters, "Dajin to Supply Transition Pieces for 1GW German Offshore Wind Farm," *TGS 4C | 4C Offshore*, November 24, 2025, https://www.tgs4c.com/NEWS/dajin-to-supply-transition-pieces-for-1gw-german-offshore-wind-farm-nid32160.html.

port of Gijón in Spain.[18] These developments matter for industrial resilience and supply-chain concentration. They should not, however, be conflated with the OEM control problem unless the supplier's role affects operational interfaces, software-dependent functions or lifecycle control of the turbine.

Investors and operators add a further layer of Chinese influence. **China Three Gorges Europe** acquired Windrose Renewables, an onshore portfolio in Spain of more than 330 MW, in 2021.[19] **CGN Europe Energy** is active in renewable projects across several Member States, including France, Ireland, Belgium, the Netherlands and Sweden, with activities that include wind farms and offshore pilot projects.[20] These cases illustrate ownership and management exposure rather than OEM control as such. However, they remain relevant because the security assessment of wind assets should consider who owns, operates and maintains the installation, and who can access the digital systems that determine its behavior over time.

3. Vulnerability analysis and the risk of "solarization"

In the early 2000s, Europe was at the forefront of solar photovoltaic panel production. However, as governments scaled back subsidies and incentives, Europe's solar manufacturing sector collapsed because it could not compete with China's massive, state-subsidized production surge. China now controls over 90% of the photovoltaic value chain while the EU accounts for just 1% of global manufacturing capacity and relies on China for 95% of its supply.

Drawing a potential analogy with wind is useful, but it should be applied carefully. In solar, Europe experienced a severe erosion of its manufacturing base under pressure from Chinese scale, public support and price competition. In wind, a similar industrial dynamic may emerge, yet the

[18] Sladjana Djunisic, "Dajin Inks MoU to Set up Offshore Wind Foundations Factory in Spain - Report," *Renewables Now,* February 2, 2026, https://renewablesnow.com/news/dajin-inks-mou-to-set-up-offshore-wind-foundations-factory-in-spain-report-1289025/.

[19] Korys, "Windrose Renewables Portfolio Sold to 'China Three Gorges Europe'," March 3, 2021, https://korys.be/pers/windrose-renewables-portfolio-sold-to-china-three-gorges-.

[20] Ibid; and Clearwater, "CGN Europe Energy Sold Two Wind Farms Totalling c.28 MW to Dutch Developer," https://www.clearwatercf.com/it/experience/transactions/cgn-europe-energy-sold-two-wind-farms-totalling-c-28-mw-to-dutch-developer/. And "Global Projects," China General Nuclear Power Group, (2025) https://en.cgnpc.com.cn/encgn/EdraPowerHoldings/pic_txt.shtml

consequences could be broader because turbines are connected cyber-physical systems rather than passive generation assets.

The level-playing-field dimension is central. In 2023, China installed around 60 GW of new wind capacity, compared with around 16 GW in Europe.[21] This scale supports manufacturing depth, supplier ecosystems and cost advantages that European firms struggle to match. If subsidized Chinese OEMs gain sustained access to European projects, the result may be a gradual weakening of European turbine manufacturing and a stronger dependence on external suppliers for assets that are central to the electricity system.

The solarization risk therefore has two dimensions:

- an industrial dimension, linked to price pressure, subsidies, manufacturing scale and loss of European capacity;
- a security dimension, linked to the fact that wind turbines depend on software, Supervisory Control and Data Acquisition (SCADA) systems, remote diagnostics, firmware updates and grid-facing control functions.

The Commission's approach to Chinese inverter technologies provides a relevant precedent. The decision to block EU funding for renewable projects involving inverters supplied by high-risk vendors such as Huawei was justified by concerns over foreign interference, access to operational data, manipulation of production parameters and remote shutdown capabilities.[22]

The wind sector is not identical to solar inverters, but the policy logic is relevant. Connected renewable infrastructure can become sensitive when external suppliers retain access to the digital functions that shape generation availability and system behavior. The evolution of Chinese clean-tech exports reinforces this concern. The value of Chinese solar PV exports to Europe peaked and then declined after 2023, a trend that can be interpreted as consistent with market saturation and price deflation after industrial erosion.[23] By contrast, Chinese wind exports to Europe are described as entering a phase

[21] Siyi Liu and Dominique Patton, "China Bans Export of Rare Earths Processing Tech over National Security," *Reuters*, December 21, 2023, https://www.reuters.com/markets/commodities/china-bans-export-rare-earths-processing-technologies-2023-12-21/.

[22] Sambell et al., *The EU's China Challenge.*

[23] "Commission blocks EU funding for Huawei solar tech", *Politico,* May 4, 2026, https://www.politico.eu/article/commission-blocks-eu-funding-for-huawei-solar-tech/

of rapid growth.[24] This does not prove that the wind sector will repeat the solar trajectory; however, it indicates that the early conditions for a similar market dynamic may be present, while the technical nature of wind assets adds a further security dimension.

4. Projective conclusion

By 2026, Chinese presence in the European wind sector has become a structural issue for industrial policy, market governance and energy security. The most immediate concern is the level-playing-field distortion created by subsidized OEMs able to compete at prices European manufacturers may find difficult to sustain. The longer-term concern is operational. As wind assets become larger, more digitalized and more integrated into the grid, the identity and risk profile of the OEM become central to security assessment.

The policy conclusion is therefore not that every Chinese component should be treated as a security risk. Instead, it is that Europe must assess whether a high-risk OEM – given its necessary and persistent influence over the turbine through embedded controllers, software updates, firmware, diagnostic systems, remote access, data interfaces and proprietary maintenance environments – should be involved in Europe's core energy infrastructure. European operation of Chinese-made wind turbines can mitigate some risks – but it cannot eliminate them entirely or sufficiently.

The next stage of the analysis should therefore move from market mapping to technical assessment. The key question is how OEM control, lifecycle dependence, and digital connectivity can translate into concrete attack paths, operational vulnerabilities, and potential system-wide effects.

[24] "China Cleantech Exports Data Explorer," *Ember Energy*, last accessed May 27, 2026, https://ember-energy.org/data/china-cleantech-exports-data-explorer/.

SECTION II: TECHNICAL ANALYSIS OF ATTACK PATHS AND SECURITY VULNERABILITIES LINKED TO CHINESE WIND TURBINES IN EUROPE

Key Takeaways

- *Strategic economic coercion may arise when an operator depends on an external OEM for spare parts, software services, diagnostic tools, updates or technical support across the turbine's operational lifecycle. Pressure does not require a direct cyberattack.*
- *Control system vulnerabilities may enable loss of visibility, altered parameters, manipulated data monitoring/transmission, unauthorized commands, or delayed responses, with possible effects on generation availability and grid management. The risk of weaponization of these vulnerabilities is particularly relevant given that Chinese companies are obliged to support, assist and cooperate with state intelligence work.*
- *Operational data can reveal asset performance, recurring faults, maintenance cycles and grid interaction, making persistent access relevant for infrastructure intelligence and for identifying weak points during a crisis.*

Chinese original equipment manufacturers, or OEMs, may create persistent exposure for European energy infrastructure through their access and influence over the turbine as an integrated asset. The relevant issue is not the origin of each component. It is the extent to which software, firmware, controllers, diagnostics, maintenance interfaces, update pathways and data access shape operational availability throughout the turbine's lifecycle.

Importantly, the existence of a material security risk does not depend on direct access to Transmission System Operator (TSO) and Distribution System Operator (DSO) control systems, substations or other grid-management infrastructure. A supplier that retains remote access capabilities and software authority over wind turbines and plant-level control functions may, in principle, influence system conditions through the generation assets themselves. The relevant question is therefore not whether the OEM can directly access the operator's network, but whether its position within the turbine architecture

could allow actions capable of affecting generation behavior, operational predictability or coordinated system response.

The analysis adopts the FAIR model, which distinguishes between loss event frequency and loss magnitude.[25] It separates direct damage from wider effects that may spread across the energy system. This is useful because the technical exposure may remain stable while the expected frequency of disruptive events changes with supplier relations, threat-actor intent and the wider political environment.

1. Technical architecture and high-impact attack paths of modern wind turbines

Modern wind turbines are cyber-physical assets. Their reliability depends on the interaction between mechanical functions, electrical conversion, control logic, connectivity and data management. Wind farms add further complexity because turbines operate within an integrated environment that includes Operational Technology networks, Supervisory Control and Data Acquisition systems (SCADA), sensors, remote diagnostics and software-update pathways.[26]

From a FAIR perspective, this architecture creates two loss channels:

- primary loss, including material damage, reduced performance or the shutdown of an individual turbine;
- secondary loss (including value of lost load, or VOLL), including prolonged outages, reduced generation capacity, grid-management difficulties or disruption of services that depend on electricity supply.

The most serious effects may arise from interconnections rather than from a single-component failure. SCADA and communications networks, if digitally compromised, can generate physical and economic consequences and spread across layers or subsystems.[27] As wind projects commonly operate for 25 to 35 years, European operators must be able to preserve oversight and

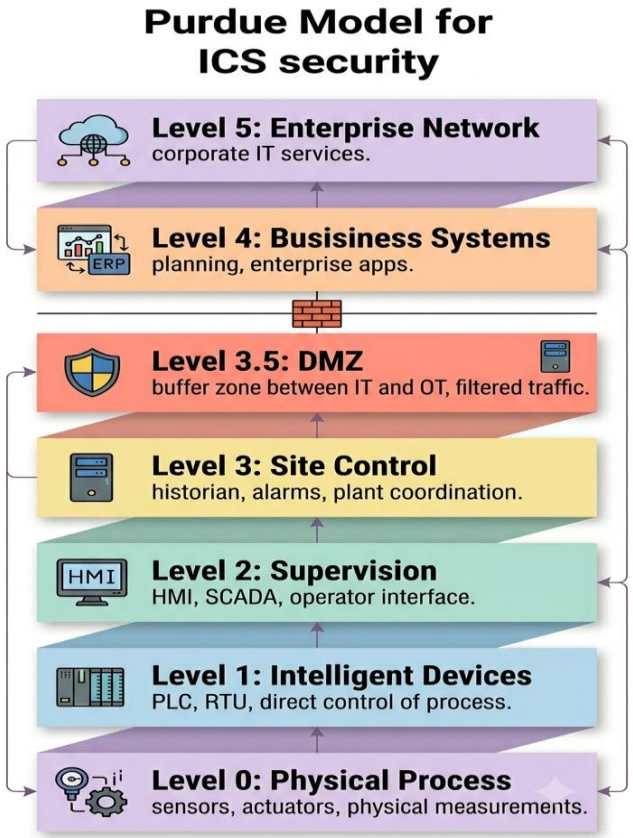
[25] Ibid

[26] "The Importance and Effectiveness of Quantifying Cyber Risk," *Fair Institute*, last accessed May 25, 2026 https://www.fairinstitute.org/what-is-fair.

[27] Office of Energy Efficiency & Renewable Energy, "Roadmap for Wind Cybersecurity," U.S. Department of Energy, (July, 2020), https://www.energy.gov/cmei/systems/articles/roadmap-wind-cybersecurity. and Meidan and Hove, *Chinese Participation in Europe's Offshore Wind Sector*

continuity of service under adverse conditions, including changes in supplier relationships, software dependencies, and threat environments.

A simplified Purdue-based model divides the turbine architecture into three connected layers. The division is analytical. In practice, the layers are interdependent, and policy measures focused on one level alone may fail to address exposure across the complete asset.[28]



1.1. Physical layer and field devices (Purdue level 0-1)

The physical layer includes blades, rotor, shaft, gearbox and braking systems. These components capture energy, convert it, and ensure structural stability. Failures can cause downtime, damage, or grid disturbances.[29] Their behavior

[28] Meidan and Hove, *Chinese Participation in Europe's Offshore Wind Sector*

[29] US Cybersecurity and Infrastructure Security Agency, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-In-Depth Strategies," (Industrial Control Systems Cyber Emergency Response Team, September 2016), https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

increasingly depends on control signals, meaning disruptions in higher layers can directly affect physical performance.

1.2. Local control systems (Purdue level 2)

This layer contains programmable logic controllers (PLCs) and turbine controllers that translate sensitive inputs into real-time control actions. It governs pitch, speed, braking, and power regulation to ensure safe and stable operation. Failures or manipulation can immediately impact turbine behavior. Reliable and determined control at this level is critical for safety and resilience.[30]

1.3. Supervisory control and digital systems (Purdue level 3-3.5)

This layer includes SCADA (supervisory control and data acquisition), Human Machine Interfaces (HMIs), communications networks, and remote-access platforms. It provides visibility, coordination, and supervisory control across turbines and wind farms. Points of weakness include remote access, updates, and system interfaces. Compromises may lead to loss of visibility, incorrect commands, or broader operational technology (OT) network impact.[31] [32]

1.4. System integration, cross-layer dependencies and high-impact attack paths

Wind turbines form part of a multi-zone architecture. External interfaces connect the perimeter zone to SCADA platforms, Operational Technology networks, local controllers, and physical systems. Sensors, controllers, and actuators link digital instructions to mechanical behavior. A compromise may therefore propagate vertically and horizontally.[33]

The most relevant cross-layer nodes are:

- interfaces between remote access, SCADA and local controllers;
- firmware and software-update processes;

[30] Ibid.

[31] Ibid.

[32] Meidan and Hove, *Chinese Participation in Europe's Offshore Wind Sector*.

[33] Office of Energy Efficiency & Renewable Energy, "Roadmap for Wind Cybersecurity".

- centralized functions such as the power plant controller;
- communications between turbines, substations and control centers;
- interfaces between electrical conversion systems and the grid.

At these nodes, a limited event may produce disproportionate effects. A communications disruption can reduce visibility across a fleet, while manipulated data monitoring and transmission, or controller anomalies can affect operational decisions, braking, pitch regulation or output. European operators strengthen resilience when they hold meaningful authority over access management, incident response, and continuity procedures. Formal responsibility for daily operations has limited value when the operator cannot verify interfaces, isolate external connections or preserve core functions without the OEM's cooperation.

The most relevant concern is not necessarily the direct compromise of grid-operator infrastructure. An OEM or other actor able to exercise influence over turbine controllers, software environments or plant-level control systems could potentially generate wider system effects through generating assets themselves. Depending on the scale and coordination of the activity, such actions could include intentional disturbances in active or reactive power output, abnormal ramping behavior, coordinated curtailment or tripping events, the creation of voltage or power oscillations, or manipulation of plant-response characteristics during periods of system stress. Unauthorized software modifications may also reduce operational predictability, weaken operator confidence in data monitoring/transmission and control signals, and complicate coordinated response measures across multiple installations.

2. Chinese exposure in critical components and weaponization potential

2.1. From component origin to control of the finished asset

Chinese exposure in the wind sector should be assessed at OEM level. A component-based approach may identify industrial dependencies, but it does not capture the operational perimeter of the turbine. The decisive question is whether the asset remains dependent on an external ecosystem for software, firmware, diagnostics, maintenance protocols, updates, remote access and data management.

This approach avoids treating every component of Chinese origin as an autonomous security concern or assuming that use of European services automatically secures the asset. European O&M, together with trusted OEMs, can mitigate exposure when it strengthens oversight, access control and continuity of service. However, its value depends on practical autonomy from the OEM's proprietary architecture. Over a 25- to 35-year operating period, the test is whether European operators can manage the turbine under adverse conditions without excessive reliance on tools, documentation or access rights controlled by the OEM.

2.2. Weaponization-enabling characteristics and strategic context

Remote monitoring, diagnostics, software updates, proprietary control systems, operational data and long-term service relationships are ordinary features of modern wind operations. When they remain insufficiently auditable or concentrated within the OEM's environment, they may create persistent channels of influence over the asset.[34] Because turbine controllers regulate pitch, rotational speed, actuators and braking systems, digital exposure can affect physical behavior.[35]

Article 7 of China's National Intelligence Law requires organizations and citizens to support, assist and cooperate with state intelligence work.[36] This does not demonstrate that commercial assets will be used for hostile purposes. It changes the risk profile when a Chinese OEM retains access to software, diagnostics, data or sensitive control functions in European energy infrastructure.

Concerns identified in adjacent energy technologies illustrate the logic. The discovery of undocumented communication devices in certain Chinese-made inverters and batteries raised questions about channels not visible to operators.[37] While the case should not be transposed automatically to wind

[34] Meidan and Hove, *Chinese Participation in Europe's Offshore Wind Sector*

[35] Global Wind Energy Council, *Mission Critical: Building the Global Wind Energy Supply Chain for a 1.5°C World*, (GWEC, 2023), https://www.gwec.net/reports/supplychain

[36] Tae-Yoon Kim et al., "With New Export Controls on Critical Minerals, Supply Concentration Risks Become Reality – Analysis - IEA," IEA, October 23, 2025, https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality

[37] Robert Freedman, "'Rogue' communication devices found on Chinese-made solar power inverters,"*Utility Dive*, May 15, 2025, https://www.utilitydive.com/news/rogue-communication-devices-found-on-chinese-made-solar-power-inverters/748242/.

turbines, it shows why access pathways, software environments and digital interfaces require scrutiny.

2.3. Why wind infrastructure is particularly exposed

Onshore and offshore wind infrastructure combines distributed generation with digital interconnection. Offshore wind farms may concentrate substantial capacity in remote assets, increasing the impact of prolonged loss of visibility or delayed repair. Onshore turbines also matter because they are increasing in size, repowering is creating market-entry opportunities, and installations may be located near sensitive infrastructure.[38]

Exposure becomes more significant when several factors converge:

- long-term dependence on proprietary interfaces and tools, spare parts, software updates and upgrades;
- remote access and update pathways that are difficult to audit fully;
- operational data that reveals performance and grid interaction;
- technical lock-in that limits substitution or independent management;
- concentrated reliance on an external OEM for continuity of service.

Delayed maintenance, support discontinuity or restricted access to tools and spare parts can reduce availability and reinforce dependence on the original supplier.[39]

3. Structured security risk assessment

3.1. Strategic economic coercion

Strategic economic coercion may arise when an operator depends on an external OEM for essential functions across the lifecycle of the installation. Pressure does not require a direct cyberattack. It may take the form of delayed spare parts, reduced technical support, interrupted software services,

[38] Emanuele Bonini, "EU Assesses Power Grid Risks from Chinese-Controlled Wind, Solar Infrastructure," *Eunews*, August 13, 2025, https://www.eunews.it/en/2025/08/13/eu-assesses-power-grid-risks-from-chinese-controlled-wind-solar-energy-infrastructure/.
and European Parliament and Council, Regulation (EU) 2024/2847, "Cyber Resilience Act," https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[39] Kosma Złotowski , "Question for Written Answer E-000889/2025 to the Commission: Chinese Wind Turbines as a Threat to Energy Security" (2025), https://www.europarl.europa.eu/doceo/document/E-10-2025-000889_EN.pdf.

selective restrictions on updates or limited access to diagnostic tools. European O&M can reduce the burden but cannot remove dependency on a trusted OEM for spare parts, software updates, upgrades and other support

3.2. Technological weaponization through control-system vulnerabilities

The second vector concerns the exploitation of control-system vulnerabilities. Wind farms depend on Industrial Control Systems (ICS) and SCADA systems, Operational Technology networks and remote-access functions.[40] Potential interference includes loss of visibility, manipulated data monitoring/transmission, unauthorized commands, altered parameters and delayed responses.

Subtle interference may be harder to detect than immediate shutdown. False data injections, sensor manipulation or delayed commands can create an apparent state of normality while the turbine operates under unsafe or inefficient conditions.[41] The Enercon and KA-SAT incident of 2022 provides an empirical reference. Around 5,800 turbines lost remote monitoring and control capabilities after a satellite communications disruption.[42] The incident did not damage the turbines physically but showed that the communications layer alone can affect operational management across a significant fleet.

3.3. Data exploitation and infrastructure intelligence

Wind farms generate continuous data on performance, maintenance cycles, faults, load response and interaction with the grid.[43] Persistent access can reveal weak points, recurring failures and the behavior of infrastructure under stress.

The location of the monitoring center does not resolve the issue. A European center may still rely on access rights, software environments or data interfaces linked to the OEM. The relevant questions still relate to data access, interface

[40] Meidan and Hove, *Chinese Participation in Europe's Offshore Wind Sector*

[41] Arsal, et al., "A Systematic Review of Cyber Risk Analysis Approaches for Wind Power Plants." *Energies* 19, no. 3:677, (2026). https://doi.org/10.3390/en19030677.

[42] Hobhouse, "The Dragon in the Grid: Limiting China's Influence in Europe's Energy System"

[43] Sarah Mcfarlane, "Ghost in the Machine? Rogue Communication Devices Found in Chinese Inverters," *Reuters*, May 14, 2025, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/

control, and whether the operator can suspend access without compromising the asset.

Offshore connectivity remains relevant because remote installations depend heavily on communications.[44] Onshore installations also require attention where proximity to sensitive infrastructure increases the value of data access. This should be treated as a risk factor, not as evidence of an established surveillance capability. Attribution is also difficult because manipulated data monitoring and transmission, or altered parameters, may resemble ordinary malfunction, delaying detection and response.

4. Plausible scenarios

The following scenarios translate the identified vectors into structured risk hypotheses. They do not predict hostile action or assume that every technical exposure will be exploited. Their purpose is to show how access, dependence and connectivity may create effects beyond the individual turbine.

4.1. Coordinated remote disruption and grid instability

The first scenario concerns simultaneous loss of visibility or control across several turbines or wind farms. The 2025 Iberian blackout showed how rapid changes in electricity-system conditions can propagate and affect wider stability, although the event resulted from a combination of technical factors rather than the scenario examined here.[45]

An actor with access to turbine-control systems, plant-level controllers, SCADA platforms or associated communications channels could seek to amplify destabilizing conditions. Disconnections-altered output or reduced visibility may hinder balancing and frequency management. The most plausible mechanisms do not require direct access to TSO or DSO control environments. A coordinated actor operating through turbine-level or plant-level control functions could instead seek to influence system conditions by

[44] WindEurope, "Wind Energy in Europe: 2024 Statistics and the Outlook for 2025-2030," (WindEurope, 2024), https://windeurope.org/data/products/wind-energy-in-europe-2024-statistics-and-the-outlook-for-2025-2030/.

[45] "Chinese Manufacturers Lead Global Wind Turbine Installations," *BloombergNEF*, March 17, 2025, https://about.bnef.com/insights/clean-energy/chinese-manufacturers-lead-global-wind-turbine-installations-bloombergnef-report-shows.

modifying the behavior of generation assets. Potential actions could include synchronized curtailment across multiple installations, abnormal ramp-rate changes, coordinated tripping of turbines, manipulation of reactive-power response or the creation of oscillatory operating patterns. The impact would depend on the scale, geographical distribution and timing of the affected assets, as well as on the resilience and response capacity of system operators. The effect would depend on the number and distribution of affected assets and the operator's response capacity.[46]

4.2. Silent data manipulation and progressive infrastructure degradation

A second scenario concerns gradual manipulation. False data injection, spoofing or interference with protection functions may cause an installation to operate outside safe parameters while available information continues to indicate apparently normal conditions.[47] Effects may include cumulative mechanical stress, incorrect maintenance decisions and delayed activation of safety systems. The incidents involving Nordex and Deutsche Windtechnik in 2022 confirm that remote-access systems and management interfaces are sensitive.[48]

4.3. Data exploitation, supply-chain pressure and impacts on critical infrastructure

A third scenario combines information access with lifecycle dependence. Operational data may reveal grid behavior and asset-level weaknesses. During a crisis, this knowledge could help identify where pressure would have the greatest effect. Delayed spare parts, reduced support, interrupted updates or restricted diagnostic access can gradually lower generation availability. The effects may extend to telecommunications, transport, ports, data centers and dual-use infrastructure.[49]

[46] Meidan and Hove, *Chinese Participation in Europe's Offshore Wind Sector*
[47] Ibid
[48] Kim et al., "With New Export Controls on Critical Minerals, Supply Concentration Risks Become Reality"
[49] Office of Energy Efficiency & Renewable Energy, "Roadmap for Wind Cybersecurity" and Arsal, et al., "A Systematic Review of Cyber Risk Analysis Approaches for Wind Power Plants."

The regulatory distinction must remain precise. The Cyber Resilience Act sets horizontal cybersecurity requirements for products with digital elements.[50] The proposed revision of the Cybersecurity Act (CSA2), discussed later in the report, addresses a different issue through a non-technical, risk-based approach to high-risk suppliers and ICT supply chains.[51] The analysis developed in this chapter supports an OEM-focused assessment because the most relevant exposure concerns *control* over the integrated asset across its lifecycle, rather than the provenance of individual *components*.

[50] "Satellite Outage Knocks out Thousands of Enercon's Wind Turbines," *Reuters*, February 28, 2022, https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/.

[51] European Commission, COM 2026/011 final, "Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)," (2026) https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

SECTION III: CHINESE COMPANIES IN EUROPE AND RESTRICTIONS ON EU COMPANIES IN THE CHINESE MARKET

Key Takeaways

- *Public sources rarely establish direct formal links between individual wind sector firms and Chinese security apparatuses, but obligations for companies under China's intelligence and cybersecurity laws elevate the risk profile given that an OEM retains access to sensitive functions.*
- *European exposure is reinforced by an asymmetry between an open European market and a Chinese system in which foreign firms operate under extensive security controls and market access constraints.*
- *The revised Cybersecurity Act (CSA2) addresses supplier risk through a broader approach to ICT supply chains and non-technical factors. A 'control not components' approach under CSA2 would be proportional one – avoiding blanket action against every Chinese industrial presence and directing scrutiny and action actors like OEMs whose technological position creates enduring operational and security risks.*

1. Chinese presence in the European wind ecosystem

Chinese participation in the European wind sector now includes OEMs, as covered in detail in Part I, as well as component suppliers, investors in renewable portfolios and operators active in broader energy infrastructure. These categories should remain distinct. Their relevance depends on the function exercised by each actor and the extent to which that function may affect industrial resilience, ownership of assets or access to the digital and operational architecture of wind turbines.[52]

Within the OEM segment, the most relevant cases are Goldwind, Envision and MingYang. The Commission's Foreign Subsidies Regulation investigation into Goldwind is an example of how the role of Chinese OEMs is increasingly

[52] Meidan and Hove, *Chinese Participation in Europe's Offshore Wind Sector*

assessed through market-integrity and economic-security considerations. Envision and MingYang have also attracted scrutiny in Europe.[53]

At the moment no general European ban on Chinese turbines exists, but individual projects may be reconsidered when security or technological-dependence concerns arise. As noted in Part I, the Waterkant project was reconsidered, moving from MingYang in favor of Siemens Gamesa.[54] MingYang is particularly significant because its presence may extend from turbine supply to industrial localization. In August 2024, MingYang, Renexia and the Italian Ministry of Enterprises and Made in Italy signed an agreement for a manufacturing plant in Italy, with an announced investment of around €500 million and up to 1,100 expected jobs.[55] But local *production* does not determine who *controls* the software, firmware, diagnostics, update pathways and interfaces of the finished asset.

Other Chinese actors raise different questions. Dajin Heavy Industry operates in offshore structures and foundations and has strengthened its European presence. This is relevant to supply-chain resilience and competition, especially because the EU has already imposed anti-dumping duties on imports of steel wind towers from China.[56] However, it should not be conflated with OEM risk unless the supplier affects the turbine's control architecture or lifecycle management.

Ownership and network infrastructure require separate assessments. As noted in detail in Part I, China Three Gorges has held positions in European wind portfolios, while CGN Europe Energy operates in renewable-energy development and management. In 2023, EDPR repurchased a 49% stake in wind portfolios in Portugal, Poland and Italy from ACE funds sponsored by China Three Gorges.[57] State Grid Corporation of China illustrates a related but distinct issue. In 2018, Germany prevented SGCC from acquiring a stake in

[53] NATO, Allied Joint Publication-3.20, "Allied Joint Doctrine for Cyberspace Operations," https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.
and Arsal, et al., "A Systematic Review of Cyber Risk Analysis Approaches for Wind Power Plants."

[54] "Nordex Hit by Cyber Security Incident, Shuts IT Systems," *Reuters*, April 2, 2022, https://www.reuters.com/technology/nordex-hit-by-cyber-security-incident-shuts-it-systems-2022-04-02/.

[55] European Parliament and the Council, Join/2022/49 final, "EU Policy on Cyber Defence," 2022, https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.

[56] EntsoE, "28 April Blackout"

[57] European Parliament and Council, Regulation (EU) 2024/2847, "Cyber Resilience Act"

50Hertz through the intervention of the public bank KfW.[58] Grid ownership concerns network governance and sensitive system information. OEM exposure concerns the turbine as a connected asset.

The distinction can be summarized as follows:

- **OEMs** raise questions about software, firmware, diagnostics, updates and operational interfaces;
- **component suppliers** primarily raise industrial-resilience and competition concerns;
- **investors and asset operators** raise questions about ownership, management and access;
- **grid-related investments** raise questions about network governance and system information.

This taxonomy matters because the same risk profile cannot be assigned to every form of Chinese presence. A supplier of offshore foundations may contribute to industrial dependence without retaining any role in digital functions. An OEM occupies a different position because it may remain linked to the asset through proprietary software, diagnostics and updates. The assessment should therefore follow the function exercised by each actor and the type of access its role makes possible.

The role of European operators should also be assessed with precision. Their involvement can mitigate exposure when it strengthens oversight, access control and continuity of service. It does not automatically remove the OEM-related risk if essential functions remain tied to proprietary tools, interfaces or update mechanisms. The relevant question is whether the operator can preserve meaningful autonomy over the asset under adverse conditions.

2. Links with Chinese security apparatuses: regulatory framework and corporate profiles

Any assessment of possible links between Chinese firms and the security apparatuses of the People's Republic of China requires caution. Public sources rarely establish direct and formalized links between individual wind-sector

[58] Patrick Criqui and Carine Sebi, "We Need to Talk about Chinese and US Influence in Europe's Energy Industry," *The Conversation*, May 7, 2024, https://theconversation.com/we-need-to-talk-about-chinese-and-us-influence-in-europes-energy-industry-227195.

firms and bodies such as the People's Liberation Army, the Ministry of State Security or the Ministry of Public Security. The analysis should distinguish direct evidence from the broader legal and institutional context.

In some cases, specific indicators exist. China General Nuclear Power was placed on the U.S. Department of Commerce Entity List and appears, together with China Three Gorges, on the U.S. Department of Defense list of Chinese military companies.[59] These designations do not automatically produce legal effects in the European Union. They remain relevant for due diligence purposes.

Ownership structures are heterogeneous:

- CGN and CTG are state-controlled enterprises under SASAC supervision;
- Goldwind has significant state-linked shareholders;
- MingYang has a fragmented and formally private ownership structure;
- Envision is founder-controlled;
- Dajin Heavy Industry has a dispersed ownership structure.

Ownership alone does not provide a complete assessment. Chinese firms operate within a legal framework that places obligations on organizations and citizens in matters of national security and intelligence. Part II notes the 2017 National Intelligence Law that requires organizations and citizens to support, assist and cooperate with state intelligence work.[60] The 2017 Cybersecurity Law reinforces this context. Article 28 requires network operators to provide technical support and assistance to public-security and state-security organs, while Article 69(3) provides sanctions for refusal.[61] These provisions affect the risk calculus when an OEM retains access to software, data or operational interfaces within European energy infrastructure.

[59] European Commission, L450/59, "Commission implementing Regulation (EU) 2021/2239 of 15 December 2021 Imposing a Definitive Anti-Dumping Duty on Imports of Certain Utility Scale Steel Wind Towers Originating in the People's Republic of China," (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R2239.

[60] European Commission, "Commission Opens In-Depth Foreign Subsidies Investigation into Goldwind's Activities in the EU Wind Sector," *European Commission Press Corner*, February 3, 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_265.

[61] Joanna Sopinska, "China's Envision and Mingyang Targeted in EU's Wind-Turbine Probe over Foreign Subsidies," *MLex*, May 23, 2024, https://www.mlex.com/mlex/articles/2179229/china-s-envision-and-mingyang-targeted-in-eu-s-wind-turbine-probe-over-foreign-subsidies

Military-civil fusion adds a broader policy dimension by encouraging closer integration between civilian industry, technological innovation and defense priorities. This does not mean that every Chinese company active in Europe has a direct relationship with the PLA, MSS or MPS. However, it does mean that the distinction between civilian and security-relevant technologies may be narrower than in other institutional environments.

The appropriate conclusion is risk-based. The assessment should consider ownership and control structure, position within the wind ecosystem, access to software and operational functions, obligations arising from the Chinese regulatory framework and the capacity of European operators to limit or suspend access. Nationality is not sufficient evidence of risk. It is equally important not to underestimate the institutional context in which OEMs operate. For wind assets, the practical test is whether European operators can verify access arrangements, restrict external connections, and sustain continuity of service without excessive dependence on the manufacturer's technical environment.

3. Chinese domestic security practices, market asymmetry and the relevance of the Cybersecurity Act 2

European exposure becomes clearer when compared with Chinese domestic security practices. The revised Cybersecurity Act proposal, known as CSA2 and presented by the Commission on 20 January 2026, reflects the growing importance of ICT supply-chain security and the possibility that risks may arise from suppliers linked to third countries that raise security concerns.[62] Its relevance for wind lies in the focus on high-risk suppliers and non-technical risk factors.

CSA2 should remain distinct from the Cyber Resilience Act, which sets horizontal cybersecurity requirements for products with digital elements. The wind-sector issue concerns the OEM's position within the complete turbine architecture. Product-level rules alone cannot capture lifecycle dependence, remote access, updates, diagnostics and data interfaces.

[62] Yun Chee Foo, "Goldwind Science Hit with EU Probe on Possible Subsidies," *Reuters*, February 3, 2026, https://www.reuters.com/sustainability/climate-energy/eu-investigate-goldwind-science-technology-possible-subsidies-2026-02-03/.

The contrast between Europe's approach and Chinese domestic practice is significant[63]. Foreign companies therefore operate in a market where access to sensitive sectors is conditioned by extensive security controls.

Market asymmetry accompanies this security asymmetry. Chinese wind policy favored domestic producers through local-content requirements, pressure for technology transfer, and market-access conditions that constrained foreign firms.[64] European companies face significant barriers in China, while Chinese firms can expand within a comparatively more open European market.

The European response should use distinctions between different instruments. Anti-dumping measures and the Foreign Subsidies Regulation address market distortion. Investment screening addresses ownership and control of sensitive assets. CSA2 may provide the basis for assessing high-risk supplier exposure in the digital and operational architecture of connected wind power plants, while preserving a proportionate distinction between commercial presence and security-relevant access.

The core conclusion is therefore precise. Europe should avoid a component-based approach that attributes risk to the origin of individual parts. The more relevant question is the persistent access an OEM retains to the functions that govern the turbine throughout its lifecycle. This access is difficult to mitigate, so the supplier's legal, corporate, and technological profile becomes directly relevant to the security of European energy infrastructure. A 'control not components' approach is a proportional one – avoiding blanket action against Chinese industrial presence and instead directing scrutiny and action towards actors like OEMs whose technological position creates enduring operational and security risks.

[63] Riham Alkousaa and Sarah Marsh, "German Company Is Set to Scrap Politically Sensitive Chinese Turbine Deal," *Reuters*, August 25, 2025, https://www.reuters.com/sustainability/climate-energy/german-company-is-set-scrap-politically-sensitive-chinese-turbine-deal-2025-08-25/.

[64] "China's MingYang Signs Italy Wind Turbine Plant Deal," *Reuters,* August 8, 2024. https://www.reuters.com/business/energy/chinas-mingyang-signs-italy-wind-turbine-plant-deal-2024-08-08/.

CeSI | CENTRO STUDI INTERNAZIONALI

CeSI - Center for International Studies is an independent think tank founded in 2004 by Andrea Margelletti, who has been its President ever since.

The activity of the Institute has always focused on the analysis of international relations and the dynamics of security and defense, with particular attention devoted to areas of crisis and the dynamics of radicalization and extremism, afterwards expanding its analytical tools also in the field of geoeconomics and conflict prevention.

The flagship of CeSI is certainly its analytical methodology which is based on an in-depth knowledge of the analised context, on a daily and transversal information research and on a periodic visit in the areas of interest, which allows the analysts of the Institute to carry out timely and dynamic work.

CONTACTS INFORMATION

Website
www.cesi-italia.org

Social
Fb: @Ce.S.I. Centro Studi Internazionali
IG: @cesi_italia
X: @CentroStudiInt
LinkedIn: Ce.S.I. Centro Studi Internazionali
Telegram: Ce.S.I. Centro Studi Internazionali

Office:
Telephone: +39 06 8535 6396
Address: Via Nomentana 251, 00161 – Rome, Italy

CeSI | CENTRO STUDI INTERNAZIONALI