Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Governing Critical Energy Infrastructure Resilience against Hybrid Threats: A Comparative Study of the European Union and Taiwan

Ondrej Voznak

600811@muni.cz

Masaryk University

Research Article

Keywords: Critical infrastructure protection, Energy security, Security governance, Hybrid threats, Infrastructure resilience

Posted Date: November 23rd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11634821/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Critical energy infrastructure is exposed to hybrid threats involving cyber operations, physical disruption, coercive pressure and supply-chain vulnerabilities. This article compares how the European Union and Taiwan govern the resilience of essential energy services under such threats. Using a structured qualitative comparison of legislation, strategies, official assessments and documented incidents, it examines prevention, preparedness, continuity, institutional coordination and recovery. The analysis identifies functional convergence despite contrasting governance systems. Both cases increasingly prioritise all-hazards risk assessment, cyber-physical coordination, continuity of essential services and recovery preparedness. The European Union primarily pursues these objectives through multilevel regulatory governance, whereas Taiwan combines national coordination, infrastructure investment by operators and whole-of-society preparedness. Differences in energy dependence and institutional authority shape the location and implementation of resilience capacities. These findings show that common security functions do not require identical institutional models. The article contributes to comparative security governance by identifying practices that may be transferable across jurisdictions while distinguishing them from context-dependent arrangements. It also highlights the limits of documentary evidence for assessing actual operational performance under simultaneous disruptions.

1. Introduction

Energy critical infrastructure has become a central security concern because the continuity of electricity, fuels, gas, and related services underpins other critical sectors and essential societal functions. Contemporary critical-infrastructure policy therefore increasingly treats energy not simply as physical assets to be protected, but as a system of services whose disruption can generate cascading effects across economies and societies (European Parliament and Council 2022a; Nikolopoulos and Makropoulos 2026; Jasiūnas et al. 2021). This shift is increasingly important as energy systems become more interconnected, digitalised, and dependent on complex supply chains, widening the range of vulnerabilities that can be disrupted or exploited. The threat environment has also changed. Energy infrastructure is exposed not only to accidents, technical failures, and natural hazards, but also to cyber operations, sabotage, coercive economic measures, information manipulation, interference with maritime or cross-border infrastructure, and supply-chain disruption (Jungwirth et al. 2023; Giannopoulos et al. 2021; Neal 2026; European Union Agency for Cybersecurity (ENISA) 2026). Hybrid threats are especially relevant because they exploit vulnerabilities across several domains and may combine physical, digital, economic, and informational instruments without necessarily crossing the threshold of armed conflict (Jungwirth et al. 2023; Giannopoulos et al. 2021). Recent work on critical energy and maritime infrastructure shows that protection is further complicated by interdependence, dispersed ownership, attribution problems, and the possibility that security measures can themselves generate operational or governance dilemmas (Jungwirth et al. 2023; Neal 2026). NIS2 likewise demonstrates that cyber risk management increasingly encompasses business continuity, incident response, recovery, and supply-chain security rather than cybersecurity in a narrow technical sense (European Parliament and Council 2022b). These developments expose the limits of approaches centred

solely on physical protection or cyber defence. Preventing disruption remains necessary, but it cannot guarantee the uninterrupted functioning of complex energy systems under uncertainty. Resilience therefore shifts attention towards the capacity to prepare for disruption, maintain essential functions, absorb consequences, restore services, and adapt after an incident (Nikolopoulos and Makropoulos 2026; Jasiūnas et al. 2021; Schmitz et al. 2025). This logic is increasingly reflected in current infrastructure policy: the EU's cable-security approach, for example, links prevention, detection, response, recovery, and deterrence within a broader resilience cycle (European Commission 2025c). Research on these issues has nevertheless developed along partly separate lines. Studies examine energy-system resilience (Jasiūnas et al. 2021; Schmitz et al. 2025), hybrid threats to critical energy infrastructure (Jungwirth et al. 2023), legal implementation of EU critical-infrastructure policy (Becker 2025), and energy resilience in Taiwan (Bui 2024). Taken together, however, this literature provides less direct comparative analysis of how different governance systems translate exposure to hybrid threats into arrangements for protecting and sustaining energy critical infrastructure. In particular, the relationship between institutional structure, energy-security conditions, and the organisation of prevention, preparedness, continuity, coordination, and recovery remains insufficiently explored across distinct political settings. The European Union and Taiwan provide a useful comparison precisely because they are not institutionally equivalent. The EU represents a multilevel regulatory system in which critical-entity resilience and cybersecurity responsibilities are distributed across Union institutions, Member States, competent authorities, and infrastructure operators (European Parliament and Council 2022a; European Parliament and Council 2022b). Taiwan, by contrast, operates through a national critical-infrastructure framework in which energy is explicitly designated as a critical sector, cybersecurity protection is coordinated through national structures, and energy and critical-infrastructure operations are incorporated into broader whole-of-society resilience arrangements (Executive Yuan 2018; Administration for Cyber Security 2026a; Office of the President 2026). Taiwan's continuing investment in grid resilience adds an operational dimension to this governance approach (Taiwan Power Company 2024). The comparison

The comparison therefore allows common security functions to be examined across contrasting institutional settings without assuming political or administrative equivalence. The article asks: How do the European Union and Taiwan translate exposure to hybrid threats into policies for protecting and strengthening the resilience of energy critical infrastructure? Two subsidiary questions guide the comparison: How are protection, preparedness, continuity and recovery incorporated into energy-infrastructure governance? Which similarities and differences emerge between the European Union and Taiwan, and what explains them? The article contributes to critical-infrastructure protection research by showing how similar resilience priorities can be implemented through different governance arrangements and by identifying which practices appear institution-specific and which may offer broader policy lessons. Section 2 establishes the conceptual relationship between energy critical infrastructure, hybrid threats, and resilience. Section 3 explains the research design, Sections 4 and 5 analyse the EU and Taiwan, Section 6 develops the comparative findings, and Section 7 concludes.

2. Energy Critical Infrastructure, Hybrid Threats and Resilience

2.1 Energy infrastructure as critical infrastructure

Critical infrastructure encompasses assets, facilities, networks and systems whose disruption would have significant consequences for the functioning of society, the economy, public safety or national security. Contemporary European policy increasingly shifts the analytical focus from individual infrastructure assets towards the critical entities that provide services essential to vital societal and economic functions (European Parliament and Council 2022a). Under the EU Critical Entities Resilience (CER) framework, energy constitutes one of the principal critical sectors, encompassing electricity, district heating and cooling, oil, gas and hydrogen. The accompanying list of essential services further emphasises that criticality derives not merely from the physical infrastructure itself, but from the functions and services whose continuity depends upon it (European Parliament and Council 2022a; European Commission 2023). Cybersecurity requirements established through the NIS2 Directive complement this approach by addressing the digital systems and networks on which essential and important entities increasingly rely (European Parliament and Council 2022b). Energy infrastructure is particularly significant because its disruption can propagate across other infrastructure sectors. Electricity, fuels and increasingly interconnected energy networks support communications, transportation, healthcare, water supply, industrial production and public administration, creating the potential for cascading and cross-sectoral effects (Becker 2025; Ouyang 2014). Energy critical infrastructure should therefore be understood as a socio-technical system rather than simply a collection of generation facilities, pipelines, grids or terminals. This perspective also connects critical infrastructure protection with the broader concept of energy security. While energy security has traditionally emphasised the uninterrupted availability of energy at an affordable price (International Energy Agency 2022), recent scholarship increasingly incorporates infrastructure vulnerability, system adaptability and resilience to shocks (Schmitz et al. 2025). Consequently,

Protecting energy infrastructure is not only a technical requirement but also a condition for maintaining essential services, economic activity and societal security.

2.2 Hybrid threats to energy critical infrastructure

The threat environment surrounding energy infrastructure extends beyond conventional accidents, natural hazards or isolated cyber incidents. Energy systems can also be deliberately targeted as part of broader strategic activities intended to exploit vulnerabilities, create uncertainty, increase economic costs or undermine the functioning of the targeted state or society (Jungwirth et al. 2023; Giannopoulos et al. 2021; Neal 2026; Dupuy et al. 2021; NATO 2024). For conceptual clarity, this article distinguishes hybrid threats from hybrid warfare. Hybrid warfare is treated as the narrower concept associated with the conduct of armed conflict through combinations of military and non-military instruments, whereas hybrid threats constitute a broader category of coordinated or strategically oriented activities that may occur below the threshold of armed conflict, during conflict, or in conjunction with other forms of interstate competition (Rauta and Monaghan 2021; Mumford and Carlucci 2023; Bergaust and Sellevåg

2024). Hybrid threats are particularly relevant to critical infrastructure because they exploit dependencies and vulnerabilities rather than relying exclusively on direct destruction. In the energy domain, relevant instruments may include cyber operations against operational or information systems, physical sabotage of pipelines, cables, substations or other facilities, manipulation of information surrounding disruptions, coercive use of energy dependencies, interference with supply chains, and combinations of these measures (Jungwirth et al. 2023; Giannopoulos et al. 2021; Neal 2026; Dupuy et al. 2021; NATO 2024). The vulnerability of maritime pipelines and undersea energy infrastructure illustrates the difficulty of attribution, surveillance and protection in environments where hostile actions may deliberately remain ambiguous (Neal 2026). The defining characteristic is therefore not a specific weapon or attack vector, but the possibility of combining different instruments across physical, digital, economic and information domains. This has important implications for protection policy.

2.3 From protection to resilience

This challenge has contributed to a broader transition from critical infrastructure protection towards critical infrastructure resilience. Protection remains essential, but it is principally concerned with preventing or reducing the probability and immediate consequences of disruption. Resilience starts from a different premise: not every disruptive event can be prevented, and no infrastructure can be protected completely against the full spectrum of natural, technological and intentional threats (Nikolopoulos and Makropoulos 2026; Council of the European Union 2022). The objective therefore becomes not only to prevent failure, but also to preserve critical functions, absorb disruption, adapt to changing conditions and restore services within an acceptable period (Nikolopoulos and Makropoulos 2026; Jasiūnas et al. 2021; Ahmadi et al. 2021; Younesi et al. 2022; Amini et al. 2023; Linkov et al. 2014). The evolution of resilience research reflects this broader understanding. Early approaches stressed robustness, redundancy, resourcefulness and rapid recovery (Linkov et al. 2014; Bruneau et al. 2003), while subsequent research increasingly incorporated organisational capabilities, interdependencies, adaptation and the continuity of essential functions (Labaka et al. 2016; Pursiainen 2018). Within energy systems, resilience is similarly

differentiated from conventional reliability. Reliability primarily concerns expected disturbances and the maintenance of normal system performance, whereas resilience becomes particularly important when systems confront severe, uncertain or unexpected disruptions that exceed routine operating assumptions (Jasiūnas et al. 2021; Ahmadi et al. 2021; Younesi et al. 2022; Amini et al. 2023; Roege et al. 2014). For the purposes of this article, resilience is therefore approached as a dynamic process encompassing protection, preparedness, continuity, response, recovery and adaptation. These stages are analytically connected rather than treated as a new formal model. Protection reduces exposure and vulnerability; preparedness establishes capacities and procedures before disruption; continuity measures seek to preserve essential services during disruption; response limits immediate consequences; recovery restores functionality; and adaptation incorporates lessons and changes that improve the system's ability to confront future disturbances (Nikolopoulos and Makropoulos 2026;

Jasiūnas et al. 2021; Labaka et al. 2016). This functional perspective is increasingly reflected in European and transatlantic policy.

(NATO 2026). Energy-system research likewise increasingly links security to the ability to withstand and recover from disturbances rather than merely preventing them (Jasiūnas et al. 2021; Schmitz et al. 2025; International Energy Agency 2020). Accordingly, resilience does not replace protection. It broadens its temporal and functional scope. For energy critical infrastructure exposed to hybrid threats, the central policy problem is therefore not simply how to prevent hostile interference, but how to ensure that strategically important energy services remain available, can be restored rapidly when disrupted, and can adapt when threat patterns and dependencies change. This understanding provides the conceptual basis for comparing how the European Union and Taiwan translate exposure to hybrid threats into the governance of energy-infrastructure resilience.

3. Research Design and Sources

3.1 Comparative design

This study adopts a qualitative comparative case-study design to examine how two institutionally different governance settings address the resilience of energy critical infrastructure under conditions of strategic pressure. Comparative case studies are particularly appropriate where the objective is not to estimate the average effect of individual variables but to examine how policies, institutions and responses are configured within their specific contexts (Yin 2018; George and Bennett 2005; Gerring 2017). The comparison follows a structured and focused logic (George and Bennett 2005): the same substantive questions are asked of both cases, while differences in institutional scale, legal authority and policy context are retained rather than artificially standardised.

The European Union and Taiwan are therefore not treated as equivalent political units. The EU represents a multilevel governance system in which competences relevant to energy, cybersecurity and critical-entity resilience are distributed across EU institutions, Member States and infrastructure operators. Taiwan is examined as a national-level governance setting in which energy security, critical-infrastructure protection and cybersecurity are organised through a different institutional architecture. This asymmetry is analytically useful because the study seeks to compare governance responses to related security problems rather than institutional forms themselves (Gerring 2017; Seawright and Gerring 2008).

3.2 Case selection

Case selection is purposive and theory-informed rather than representative (Gerring 2017; Seawright and Gerring 2008). The EU and Taiwan were selected because both confront significant questions of energy security and infrastructure resilience while differing substantially in geography, institutional organisation and energy-policy governance. Five considerations guided selection: strategic exposure to external pressure; the centrality of energy security to economic and societal functioning; dependence on externally connected energy supplies and supply chains; explicit policy attention to critical-infrastructure

protection; and contrasting institutional arrangements. These characteristics create sufficient common ground for meaningful comparison without if identical threats produce identical policy responses. The resulting design is intended to identify similarities, differences and context-dependent explanations, not to generalise statistically from two cases.

3.3 Sources

The analysis relies on triangulation across academic and primary documentary sources (Yin 2018; Bowen 2009; Schreier 2012). Peer-reviewed research provides the conceptual and empirical background, while primary sources establish the formal policy and governance arrangements in each case. The documentary corpus primarily covers the period from 2017 to 24 September 2026, capturing the most recent development of critical-infrastructure, cybersecurity, energy-security, and resilience policies in both cases. Earlier documents were retained where necessary to establish institutional or conceptual continuity. Documents were included when they directly addressed energy critical infrastructure, critical-entity protection, cybersecurity, preparedness, continuity of essential services, crisis response, recovery, or closely related energy-security measures. Primary official sources were prioritised wherever available, while peer-reviewed literature was used to contextualise, interpret, and cross-check formal policy developments. For the EU, the corpus includes the Critical Entities Resilience Directive, NIS2, Council recommendations on critical-infrastructure resilience and cross-border disruption, European Commission policy documents, ENISA assessments, and relevant energy-security materials (European Parliament and Council 2022a; European Parliament and Council 2022b; Council of the European Union 2022; Council of the European Union 2024; European Union Agency for Cybersecurity (ENISA) 2024; European Commission 2026a).

(International Energy Agency 2025). Official incident reports are included where they provide sufficiently documented evidence relevant to infrastructure disruption or institutional response.

3.4 Analytical procedure

Documents are analysed qualitatively and comparatively, drawing on established approaches to document and qualitative content analysis (Bowen 2009; Schreier 2012). The analysis proceeds in two stages. First, each case is examined independently to reconstruct the relevant governance architecture, policy priorities and measures concerning energy critical infrastructure. Second, findings are compared across five recurring dimensions: prevention, preparedness, continuity, institutional coordination, and recovery. These dimensions are used solely to organise the comparison. They are not treated as a new resilience model, converted into indicators, assigned scores or combined into an index. The purpose is to ensure that equivalent questions are asked of both cases while allowing institutionally specific practices to remain visible. Attention is also paid to temporal change, particularly where policies were revised in response to emerging cyber, physical, supply-chain or geopolitical risks. The comparative discussion therefore focuses on which resilience priorities converge, where governance responses diverge, and how differences in institutional structure, energy dependence and strategic exposure help explain those patterns.

4. European Union: Protecting Energy Critical Infrastructure

4.1 Evolution of EU critical infrastructure protection EU critical-infrastructure policy has progressively moved from the protection of designated physical assets towards a broader resilience-oriented approach centred on the continued provision of essential services. The earlier European Critical Infrastructure framework primarily focused on the identification and protection of infrastructure whose disruption could have significant cross-border effects. The Critical Entities Resilience (CER) Directive substantially broadens this logic by focusing on critical entities, essential services and an all- hazards understanding of risk (European Parliament and Council 2022a; European Commission 2026b). Energy is one of the core sectors covered, including electricity, gas, oil, district heating and cooling, and hydrogen (European Parliament and Council 2022a; European Commission 2023). The CER Directive requires Member States and critical entities to assess relevant natural and human-induced risks, explicitly including hybrid and other antagonistic threats, cross-border risks and cross-sectoral dependencies (European Parliament and Council 2022a). Critical entities must adopt proportionate technical, security and organisational measures covering prevention, physical protection, response, mitigation, business continuity and recovery (European Parliament and Council 2022a).

The physical-resilience framework is complemented by NIS2, which strengthens cybersecurity risk management and incident reporting across critical sectors, including energy (European Parliament and Council 2022b). Importantly, NIS2 itself applies an all-hazards logic and addresses supply-chain security alongside incident prevention, detection, response and recovery (European Parliament and Council 2022b). Energy-specific instruments add another layer. Regulation (EU) 2019/941 requires electricity crisis scenarios and national, regional and bilateral risk-preparedness plans (European Parliament and Council 2019), while Regulation (EU) 2017/1938 provides mechanisms for gas-supply preparedness, emergency response and solidarity (European Parliament and Council 2017). The 2024 electricity cybersecurity network code further establishes common requirements for cybersecurity risk assessment, planning, monitoring, reporting and crisis management in cross-border electricity flows (European Commission 2024).

4.2 Changing threat environment

This regulatory evolution reflects a threat environment in which disruption may originate simultaneously from physical, cyber, technological, environmental and geopolitical sources. EU assessments increasingly emphasise the interaction between digitalisation, infrastructure interdependence and hostile activities (European Union Agency for Cybersecurity (ENISA) 2024; European Union Agency for Cybersecurity (ENISA) 2025). ENISA reports a cybersecurity environment shaped by cybercrime, hacktivism, espionage and geopolitically motivated activity, with entities classified under NIS2 constituting a substantial share of affected organisations (European Union Agency for Cybersecurity (ENISA) 2026; European Union Agency for Cybersecurity (ENISA) 2025). Physical infrastructure has simultaneously gained greater policy attention. Submarine electricity cables, interconnectors, pipelines and offshore energy assets create strategic benefits through market integration and diversification but

also introduce geographically dispersed and difficult-to-protect points of vulnerability (European Commission 2025f). The 2025 EU Action Plan on Cable Security consequently addresses submarine electricity and communication cables through an entire resilience cycle encompassing prevention, detection, response, recovery and deterrence (European Commission 2025f). Subsequent EU risk assessment and stress-testing activities have reinforced this emphasis on dependencies and cross-border consequences (European Commission 2025f; European Commission 2026c). Supply security constitutes a further dimension.

4.3 Energy infrastructure resilience governance EU energy-infrastructure governance increasingly reflects several mutually reinforcing functions. Prevention is addressed through entity-level risk assessments, physical and organisational security measures, cybersecurity requirements and sector-specific risk identification (European Parliament and Council 2022a; European Parliament and Council 2022b; European Commission 2024). The CER framework explicitly requires measures designed to prevent incidents, while NIS2 extends preventive obligations into digital systems and supply chains (European Parliament and Council 2022a; European Parliament and Council 2022b). Preparedness is embedded particularly strongly in the electricity and gas sectors. Electricity risk-preparedness plans must identify crisis scenarios, responsibilities, communication procedures and national, regional and bilateral measures (European Parliament and Council 2019). Gas-security rules similarly combine preventive planning with mechanisms for coordinated action during supply

disruptions (European Parliament and Council 2017). At the broader level, the European Preparedness Union Strategy calls for greater anticipation, risk assessment, stress testing and preparedness across critical societal functions (European Commission and High Representative 2025b). Continuity constitutes a central link between protection and resilience. CER requires critical entities to consider business-continuity measures and alternative supply chains so that essential services can be maintained or resumed following disruption (European Parliament and Council 2022a). In energy policy, storage, system interconnection, alternative supply routes, redundancy and diversification perform comparable functions by reducing dependence on individual infrastructure components or suppliers (European Commission 2022; European Commission 2025d). Coordination is particularly important because EU energy infrastructure crosses jurisdictional and sectoral boundaries. CER establishes cooperation among national authorities and at Union level (European Parliament and Council 2022a), while the Commission’s 2026 guidance elaborates non-binding resilience measures (European Commission 2026a), while the Critical Infrastructure Blueprint provides procedures for situational awareness, information sharing and coordinated responses to disruptions with significant cross-border relevance (Council of the European Union 2024). The electricity cybersecurity network code similarly links energy authorities, cybersecurity bodies, system operators and existing structures such as CSIRTs and EU-CyCLONe (European Commission 2024).

4.4 Strengths, vulnerabilities and unresolved challenges

The principal strength of the EU approach is therefore its increasingly layered and all-hazards architecture. Physical protection, cybersecurity, supply security, preparedness and crisis coordination are

no longer treated as entirely separate policy fields (European Parliament and Council 2022a; European Parliament and Council 2022b; European Parliament and Council 2019; European Parliament and Council 2017; European Commission 2024). The framework also recognises that resilience depends on essential functions and interdependencies rather than solely on individual installations. However, this architecture creates its own governance challenges. Implementation remains distributed among EU institutions, Member States, regulators and predominantly public or private infrastructure operators. Delayed national implementation of both CER and NIS2 has illustrated uneven implementation capacity: in 2025 the Commission pursued infringement procedures against multiple Member States for incomplete transposition (European Commission 2025a; European Commission 2025b). Cross-border interdependence also means that resilience achieved within one jurisdiction may remain vulnerable to weaknesses elsewhere. The emerging EU approach can consequently be characterised as a transition from infrastructure protection towards system-level resilience, but not as a completed process.

5. Taiwan: Protecting Energy Critical Infrastructure

Protecting Energy Critical Infrastructure

5.1 Energy security and critical infrastructure context

Taiwan treats energy infrastructure as an explicit component of national critical infrastructure. The Executive Yuan’s Guidelines for National Critical Infrastructure Protection define critical infrastructure broadly as physical or virtual assets, systems and networks whose disruption could impair government and societal functions, generate economic losses or damage national security and interests (Executive Yuan 2018). The national framework distinguishes nine critical-infrastructure sectors, with energy encompassing electricity, petroleum and natural gas (Executive Yuan 2018; Administration for Cyber Security 2026a). Critical Information Infrastructure supporting core infrastructure functions is incorporated within this architecture rather than treated as an entirely separate system (Executive Yuan 2018). Energy infrastructure acquires strategic significance because Taiwan combines an islanded energy system with heavy dependence on imported fuels. The Energy Administration identifies dependence on external energy supplies as a persistent energy-security concern (Energy Administration 2026; Energy Administration 2023). Recent government policy therefore combines diversification of suppliers, contractual arrangements, statutory inventories, domestic renewable generation and infrastructure investment as complementary means of maintaining energy supply (Ministry of Economic Affairs 2026b; Ministry of Economic Affairs 2026c). Energy resilience has consequently become intertwined with broader national resilience.

5.2 Threat environment Taiwan's energy infrastructure operates in an environment where natural, technological, cyber and intentional disruptions can interact. Earthquakes and typhoons remain significant operational hazards. During the April 2024 Hualien earthquake, generation facilities were affected and more than 370,000 customers temporarily lost power, while several typhoons during the

same year further tested restoration capabilities (Taiwan Power Company 2024). Such events reinforce the importance of redundancy, distributed infrastructure and rapid repair independently of intentional security threats. Cyber risk constitutes a second dimension. Critical infrastructure providers are subject to Taiwan's cybersecurity regime, while the Administration for Cyber Security coordinates joint defence arrangements connecting responsible sectoral authorities, Information Sharing and Analysis Centers, Computer Emergency Response Teams and Security Operation Centers (Administration for Cyber Security 2026a; Republic of China (Taiwan) 2022). Government reporting continues to record significant volumes of intrusion attempts and other malicious activities, including incidents affecting equipment relevant to physical access and infrastructure operations (Administration for Cyber Security 2025; Administration for Cyber Security 2026b).

Intentional physical disruption is incorporated into the national protection framework as well. The national critical-infrastructure protection framework addresses intentional disruption through preventive measures and institutional coordination (Executive Yuan 2026a). At the same time, the dependence of oil and LNG supplies on maritime transportation creates exposure to external supply interruptions. Government responses emphasise diversification of suppliers and transport arrangements, safety stocks, alternative procurement and contingency planning rather than reliance on a single protective measure (Ministry of Economic Affairs 2026b; Ministry of Economic Affairs 2026c; Ministry of Economic Affairs 2026d). The threat environment is therefore multidimensional: resilience must address failures within infrastructure, attacks upon it and disruptions to the external flows on which its operation depends.

5.3 Energy infrastructure resilience governance Taiwan's approach can similarly be examined through prevention, preparedness, continuity, coordination and recovery. Prevention begins with the national CI protection framework. Responsible authorities require critical-infrastructure providers to identify assets and vulnerabilities, conduct all-hazards risk assessments and establish security protection plans containing both improvement and emergency-response measures (Executive Yuan 2026a). Cybersecurity obligations complement physical protection through provider designation, security-management requirements and national-level information sharing (Administration for Cyber Security 2026a; Republic of China (Taiwan) 2022). Preparedness combines infrastructure planning with exercises and contingency arrangements. The Homeland Security Policy Committee requires response procedures contained in infrastructure protection plans to be tested through practical exercises and continuously reviewed (Executive Yuan 2026a). This approach has increasingly been integrated with whole-of-society preparedness, including exercises intended to verify central-government, local-government and private-sector capacities under severe scenarios (Office of the President 2026; Office of the President 2024). Continuity is especially visible in energy supply and electricity policy. Natural-gas importers are legally required to maintain minimum storage capacity and safety inventories; the minimum safety stock applicable in 2025–2026 is eleven days and is scheduled to increase to fourteen days from 2027 (Ministry of Economic Affairs 2026e). Supplier diversification, long-term contracting and contingency procurement complement these inventories (Ministry of Economic Affairs 2026c). Within the electricity system, Taipower's Grid Resilience Enhancement Program represents a major structural investment in

decentralisation, reinforcement and system defence. The programme involves approximately NT$564.5 billion in planned investment and seeks to reduce risks generated by excessive grid concentration (Taiwan Power Company 2024; Taiwan Power Company 2026a). Grid development also provides mechanisms for continuity and adaptation. Distributed grids, microgrids, energy storage, equipment renewal and enhanced system defence are intended to localise failures, maintain regional supply and facilitate restoration (Taiwan Power Company 2026a; Taiwan Power Company 2026b; Taiwan Power Company 2026c). By the end of 2024, 98 projects under the resilience programme had been completed, while deployment of digital substations, storage and distributed-energy management continued (Taiwan Power Company 2024; Taiwan Power Company 2026a). Coordination operates through several overlapping mechanisms.

5.4 Strengths, vulnerabilities and unresolved challenges

Taiwan's principal strength is the close connection between infrastructure protection and operational continuity. Grid decentralisation, emergency exercises, cybersecurity coordination, fuel inventories and recovery arrangements demonstrate that resilience is increasingly approached as the capacity to sustain and restore critical functions rather than simply prevent damage (Taiwan Power Company 2024; Executive Yuan 2026a; Taiwan Power Company 2026a; Executive Yuan 2026b). Compared with a purely asset-based protection approach, this creates a comparatively strong operational emphasis. Important vulnerabilities nevertheless remain. High dependence on maritime energy imports cannot be eliminated through physical protection of domestic infrastructure, while greater use of digital control, smart grids and distributed systems expands the cyber-physical attack surface (Administration for Cyber Security 2026a; Ministry of Economic Affairs 2026b; Republic of China (Taiwan) 2022). Grid resilience investments also require long implementation periods, and diversification of suppliers does not remove dependence on maritime transportation itself. Recent research similarly identifies energy sufficiency and system response capacity as central determinants of Taiwanese energy resilience (Bui 2024). Taiwan can therefore be characterised as moving from critical-infrastructure protection towards integrated national resilience, but through a path distinct from that of the EU.

6. Comparative Discussion

6.1 Converging resilience priorities

The comparison demonstrates substantial convergence in how the European Union and Taiwan understand the functions required to protect energy critical infrastructure, despite major differences in their institutional structures and strategic environments. In both cases, resilience increasingly extends beyond preventing damage to individual assets. Policy attention encompasses preparedness before disruption, continuity of essential services during disruption, coordination among responsible authorities and operators, and recovery after critical functions have been degraded (European Parliament and Council 2022a; Executive Yuan 2018; Executive Yuan 2026a). This corresponds with the broader

evolution of critical- infrastructure resilience from asset protection towards sustaining essential societal functions (Nikolopoulos and Makropoulos 2026; Labaka et al. 2016). The convergence is particularly visible in three areas. First, both cases increasingly adopt an all-hazards perspective. The EU CER framework explicitly addresses natural and human- induced, accidental and intentional risks, while Taiwan's critical-infrastructure system similarly requires identification of vulnerabilities and all-hazards risk assessment (European Parliament and Council 2022a; Executive Yuan 2026a). Neither system therefore structures resilience around a single anticipated attack vector.

Second, physical and cyber resilience are becoming institutionally interconnected. CER and NIS2 create complementary physical and cybersecurity obligations within the EU, reinforced by sector-specific requirements for electricity (European Parliament and Council 2022a; European Parliament and Council 2022b; European Commission 2024). Taiwan similarly connects national critical-infrastructure protection with cybersecurity structures linking competent authorities, infrastructure providers, information-sharing mechanisms and incident-response capabilities (Administration for Cyber Security 2026a; Republic of China (Taiwan) 2022). Third, continuity increasingly acts as the bridge between security and resilience. EU measures emphasise business continuity, redundancy, alternative supply chains and restoration of essential services (European Parliament and Council 2022a). Taiwan combines infrastructure protection with grid decentralisation, system defence, emergency procedures, fuel inventories and restoration capacity (Taiwan Power Company 2024; Ministry of Economic Affairs 2026e; Taiwan Power Company 2026a; Executive Yuan 2026b). The resulting convergence is therefore functional rather than institutional: both systems increasingly seek to prevent disruption where possible while retaining the capacity to continue, restore and adapt when prevention fails.

6.2 Different institutional responses

Similar resilience priorities are translated into markedly different governance arrangements. The EU response is characterised by multilevel regulatory governance. Resilience requirements are established through EU legislation and sector-specific instruments but implemented through Member States, national competent authorities and infrastructure operators (European Parliament and Council 2022a; European Parliament and Council 2022b; European Parliament and Council 2019; European Parliament and Council 2017; European Commission 2024). Cross- border coordination is consequently an inherent part of the system because electricity networks, gas infrastructure, supply chains and digital dependencies frequently extend beyond individual jurisdictions (Council of the European Union 2024; European Commission 2026c). This architecture provides common minimum requirements across a large integrated space but also makes implementation dependent on coordination among multiple levels of authority. Difficulties and delays in transposing CER and NIS2 illustrate that adoption of common rules does not automatically generate uniform operational capability (European Commission 2025a; European Commission 2025b). EU resilience governance therefore combines regulatory harmonisation with continuing variation in national implementation. Taiwan operates through a more territorially concentrated governance structure.

6.3 Energy dependence and strategic exposure

Energy dependence further shapes the location of resilience efforts. Both systems depend on external energy relationships, but the structure of that dependence differs significantly. EU policy has increasingly sought to reduce vulnerability through supplier diversification, storage, infrastructure interconnection, alternative routes and greater integration of energy markets (European Parliament and Council 2017; European Commission 2022; European Commission 2025d). Because the European energy system spans multiple states and external connections, resilience can partly be generated through geographical diversification, cross-border infrastructure and mutual support mechanisms. Taiwan's geographical conditions constrain the same options. High reliance on imported fuels combined with maritime transportation means that diversification of suppliers does not remove dependence on external sea-borne flows (Energy Administration 2026; Energy Administration 2023; Ministry of Economic Affairs 2026b; Ministry of Economic Affairs 2026c). Consequently, supply resilience places greater emphasis on inventories, contractual diversification, contingency procurement and domestic system preparedness (Ministry of Economic Affairs 2026c; Ministry of Economic Affairs 2026e).

6.4 What travels across cases?

The comparison consequently distinguishes between context-dependent arrangements and potentially transferable resilience practices. Institutional structures themselves are poorly transferable. The EU's supranational regulatory architecture reflects the distribution of authority between EU institutions and Member States, while Taiwan's central coordination and whole- of-society arrangements reflect a substantially different political, geographical and infrastructure context (European Parliament and Council 2022a; Office of the President 2026). Specific requirements concerning gas inventories, cross-border solidarity or grid organisation similarly respond to energy-system characteristics (European Parliament and Council 2019; European Parliament and Council 2017). Several underlying practices, however, appear less dependent on institutional form. The first is the shift from protecting assets towards maintaining essential functions. Both cases demonstrate the value of identifying which services must continue even when individual components fail (European Parliament and Council 2022a; Executive Yuan 2018; Executive Yuan 2026b). Second, all-hazards assessment allows governance systems to address cyber, physical, natural and supply-related disruption without constructing separate resilience systems for every threat category (European Parliament and Council 2022a; Executive Yuan 2026a).

cyber institutions and infrastructure operators differ organisationally but share the recognition that coordination cannot be improvised only after an incident (Administration for Cyber Security 2026a; Council of the European Union 2024; European Commission 2024; Republic of China (Taiwan) 2022). Regular exercises and testing similarly translate formal preparedness into operational capability (European Parliament and Council 2019; European Commission and High Representative 2025b; Office of the President 2024; Executive Yuan 2026a). Finally, both cases indicate the importance of treating recovery as part of preparedness rather than as a separate post-crisis activity. Repair capacity, restoration priorities, redundancy and adaptation determine whether disruption becomes a temporary loss of service or a prolonged systemic failure (Taiwan Power Company 2026a; Executive Yuan 2026b). The principal comparative finding is therefore not that one governance system offers a template for the

other. Rather, effective resilience appears to depend on translating common functional priorities into arrangements compatible with specific institutional structures, infrastructure configurations and patterns of energy dependence. For critical-infrastructure policy, the transferable lesson lies less in replicating institutions than in ensuring that protection, preparedness, continuity, coordination and recovery form a connected governance process.

7. Conclusions

This article examined how the European Union and Taiwan translate exposure to hybrid threats into policies for protecting and strengthening the resilience of energy critical infrastructure. The comparison shows that both cases have moved beyond a narrow understanding of infrastructure protection centred on preventing physical damage or isolated cyber incidents. Instead, resilience governance increasingly combines prevention, preparedness, continuity of essential services, institutional coordination, response and recovery (European Parliament and Council 2022a; Executive Yuan 2018; Executive Yuan 2026a). The principal answer to the research question is therefore that both governance systems respond to hybrid and other complex threats by broadening the objective of critical-infrastructure policy from protecting individual assets towards sustaining and restoring essential energy functions under disruption. Four principal findings emerge from the comparison. First, the EU and Taiwan display substantial functional convergence. Despite their different political and institutional structures, both increasingly rely on all-hazards risk assessment, cybersecurity and physical protection, continuity arrangements, emergency preparedness and recovery mechanisms (European Parliament and Council 2022a; European Parliament and Council 2022b; Administration for Cyber Security 2026a; Executive Yuan 2026a). Second, this convergence does not imply institutional uniformity.

settings even where legal systems, institutional structures and energy configurations differ substantially (European Parliament and Council 2022a; Executive Yuan 2026a; Executive Yuan 2026b). Conceptually, the article contributes to the literature on critical-infrastructure resilience by reinforcing the distinction between protection and resilience. Protection remains indispensable, but resilience extends the analytical horizon beyond preventing incidents towards maintaining, restoring and adapting essential functions after disruption occurs (Nikolopoulos and Makropoulos 2026; Jasiūnas et al. 2021; Labaka et al. 2016). The comparison further suggests that resilience should not be understood as a single institutional template. Similar functional objectives can be implemented through different governance arrangements. What matters analytically is therefore less whether jurisdictions adopt identical institutional structures than whether protection, preparedness, continuity, coordination and recovery are effectively connected. This finding also has practical implications. Policymakers should be cautious about transferring entire institutional arrangements between jurisdictions. Measures that depend on supranational regulation, geographic interconnection or specific energy-market structures may not travel easily. By contrast, practices such as tested continuity procedures, redundancy, cross-agency coordination, information sharing, recovery planning and regular exercises are less dependent on institutional form and may therefore offer broader lessons for critical-infrastructure governance (Council of the European Union 2024; European Commission 2024; Office of the President 2024; Executive Yuan

2026a). The comparison also underlines the need to treat energy security and infrastructure resilience as interconnected policy fields rather than separate domains. Several limitations should nevertheless be acknowledged.

Declarations

Author Contribution

O.V. was responsible for the conceptualization and design of the study, methodology, collection and analysis of documentary evidence, comparative analysis, interpretation of findings, and preparation of the original manuscript. O.V. critically reviewed and revised the manuscript, approved the final version for submission, and accepts full responsibility for the integrity and accuracy of the work.

Data availability: The analysis draws on publicly available institutional documents and published sources identified in the reference list. No original interview or restricted-access dataset is analysed.

References

1. Administration for Cyber Security (2025) Cybersecurity Monthly Report (June), Taipei, 2025.
2. Administration for Cyber Security (2026a) Cyber Security Defense of Critical Infrastructure. Ministry of Digital Affairs, Taipei. https://web.moda.gov.tw/en/ACS/operations/ciip/650
3. Administration for Cyber Security (2026b) Cybersecurity Monthly Report (May), Taipei, 2026.
4. Ahmadi S, Saboohi Y, Vakili A (2021) Frameworks, quantitative indicators, characters, and modeling approaches to analysis of energy system resilience: A review, Renew. Sustain. Energy Rev. 144 () 110988, https://doi.org/10.1016/j.rser.2021.110988.
5. Amini F, Ghassemzadeh S, Rostami N, Tabar VS (2023) Electrical energy systems resilience: A comprehensive review on definitions, challenges, enhancements and future proceedings, IET Renew. Power Gener. 17 () 1835–1858, https://doi.org/10.1049/rpg2.12705.
6. Becker M (2025) Transposing EU-legislation on critical infrastructure protection: Legal implementation performance in the Baltic Sea region, Int. J. Crit. Infrastruct. Prot. 50 () 100781, https://doi.org/10.1016/j.ijcip.2025.100781.
7. Bergaust JC, Sellevåg SR (2024) Improved conceptualising of hybrid interference below the threshold of armed conflict, Eur. Secur. 33 () 169–195, https://doi.org/10.1080/09662839.2023.2267478.
8. Bowen GA (2009) Document analysis as a qualitative research method, Qual. Res. J. 9 () 27–40, https://doi.org/10.3316/QRJ0902027.
9. Bruneau M, Chang SE, Eguchi RT (2003) et al., A framework to quantitatively assess and enhance the seismic resilience of communities, Earthq. Spectra 19 () 733–752, https://doi.org/10.1193/1.1623497.

10. Bui T-D, Kumpimpa T, Lin C-WR, Lim MK, Tseng M-L (2024) Assessing energy resilience under uncertainty in Taiwan: System response ability and energy sufficiency, Energy Strategy Rev. 53 () 101403, https://doi.org/10.1016/j.esr.2024.101403.
11. Council of the European Union (2022) Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, 2023/C 20/01, Off. J. Eur. Union C 20 (2023) 1–11.
12. Council of the European Union (2024) Council Recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance, C/2024/4371, Off. J. Eur. Union (2024).
13. Dupuy AC, Nussbaum D, Butrimas V, Granitsas A (2021) Energy security in the era of hybrid warfare, NATO Review, 13 January.
14. Energy Administration (2023) What Is the Current Status of International Energy Cooperation Involving Taiwan? What Is the Prospect of the Cooperation?, Taipei, updated 7 June.
15. Energy Administration (2026) Energy Statistics Handbook, Taipei, updated.
16. European Commission (2022) REPowerEU Plan, COM(2022) 230 final, Brussels, 2022.
17. European Commission (2023) Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 supplementing Directive (EU) 2022/2557 by establishing a list of essential services, Off. J. Eur. Union (2023).
18. European Commission (2024) Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 by establishing a network code on sector- specific rules for cybersecurity aspects of cross-border electricity flows, Off. J. Eur. Union (2024).
19. European Commission (2025a) Commission Calls on 19 Member States to Fully Transpose the NIS2 Directive, Brussels, 7 May.
20. European Commission (2025b) July Infringements Package: Critical Entities Resilience Directive, Brussels, 17 July.
21. European Commission (2025c) ProtectEU: A European Internal Security Strategy, COM(2025) 148 final, Strasbourg, 2025.
22. European Commission (2025d) Roadmap towards ending Russian energy imports, COM(2025) 440 final, Strasbourg, 6 May 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0440
23. European Commission (2025e) State of the Energy Union Report, Brussels, 2025.
24. European Commission (2025f) Submarine Cable Infrastructures Expert Group, Report on Security and Resilience of EU Submarine Cable Infrastructures, Brussels.
25. European Commission (2026a) Communication from the Commission – Guidelines on the application of Article 13(5) of Directive (EU) 2022/2557 on the resilience of critical entities, C/2026/3712, Off. J. Eur. Union, 13 July 2026.

26. European Commission (2026b) Critical Infrastructure and Cybersecurity, Directorate-General for Energy, Brussels, updated.
27. European Commission (2026c) Critical Infrastructure Resilience at EU-Level, Directorate- General for Migration and Home Affairs, Brussels.
28. European Commission (2026d) Submarine Cable Security Toolbox and Cable Projects of European Interest, Brussels.
29. European Commission and High Representative (2025a) EU Action Plan on Cable Security, JOIN(2025) 9 final, Brussels, 21 February 2025.
30. European Commission and High Representative (2025b) European Preparedness Union Strategy, JOIN(2025) 130 final, Brussels, 26 March 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0130
31. European Parliament and Council (2017) Regulation (EU) 2017/1938 of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, Off. J. Eur. Union L 280 (2017) 1–56.
32. European Parliament and Council (2019) Regulation (EU) 2019/941 of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, Off. J. Eur. Union L 158 (2019) 1–21.
33. European Parliament and Council (2022a) Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Off. J. Eur. Union L 333 (2022) 164–198.
34. European Parliament and Council (2022b) Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Off. J. Eur. Union L 333 (2022) 80–152.
35. European Union Agency for Cybersecurity (ENISA) (2024) Report on the State of the Cybersecurity in the Union, ENISA, Athens, 2024.
36. European Union Agency for Cybersecurity (ENISA) (2025) ENISA Threat Landscape, ENISA, Athens, 2025.
37. European Union Agency for Cybersecurity (ENISA) (2026) ENISA Threat Landscape, ENISA, Athens, 2026.
38. Executive Yuan (2018) Guidelines for National Critical Infrastructure Protection, Taipei, revised 18 May.
39. Executive Yuan (2026a) Prevention: National Critical Infrastructure Security Protection, Taipei.
40. Executive Yuan (2026b) Response and Recovery of Critical Infrastructure, Taipei.
41. George AL, Bennett A (2005) Case Studies and Theory Development in the Social Sciences, MIT Press, Cambridge, MA.

42. Gerring J (2017) Case Study Research: Principles and Practices, second ed., Cambridge University Press, Cambridge.
43. Giannopoulos G, Smith H, Theocharidou M (2021) The Landscape of Hybrid Threats: A Conceptual Model, Publications Office of the European Union, Luxembourg,, EUR 30585 EN, https://doi.org/10.2760/44985.
44. International Energy Agency (2020) Power Systems in Transition: Challenges and Opportunities Ahead for Electricity Security, IEA, Paris.
45. International Energy Agency (2022) World Energy Outlook, IEA, Paris, 2022.
46. International Energy Agency (2025) World Energy Outlook, IEA, Paris, 2025.
47. Jasiūnas J, Lund PD, Mikkola J (2021) Energy system resilience – A review, Renew. Sustain. Energy Rev. 150 () 111476, https://doi.org/10.1016/j.rser.2021.111476.
48. Jungwirth R, Giannopoulos G, Valsamos G (2023) et al., Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, Publications Office of the European Union, Luxembourg,, EUR 31505 EN, https://doi.org/10.2760/58406.
49. Labaka L, Hernantes J, Sarriegi JM (2016) A holistic framework for building critical infrastructure resilience, Technol. Forecast. Soc. Change 103 () 21–33, https://doi.org/10.1016/j.techfore.2015.11.005.
50. Linkov I, Bridges T, Creutzig F (2014) et al., Changing the resilience paradigm, Nat. Clim. Change 4 () 407–409, https://doi.org/10.1038/nclimate2227.
51. Ministry of Economic Affairs (2026a) Domestic Energy Supply Remains Sufficient amid Geopolitical Disruption, Taipei, 2 March.
52. Ministry of Economic Affairs (2026b) Energy Transition Promotion Scheme: Developing Diversified Green Energy, Promoting Deep Energy Saving, Deploying Technical Power Storage and Strengthening Power Grid Resilience, Taipei.
53. Ministry of Economic Affairs (2026c) Government Continues Diversified Procurement and Renewable Energy Development to Strengthen Energy Supply Resilience, Taipei, 13 August.
54. Ministry of Economic Affairs (2026d) No Domestic Power or Gas Shortages Since the Middle East Conflict; Natural Gas Dispatches Has Been Well Managed, Taipei, 15 April.
55. Ministry of Economic Affairs (2026e) Required Storage Capacity for Natural Gas Production and Import Enterprises, Laws and Regulations Retrieving System, Taipei.
56. Mumford A, Carlucci P (2023) Hybrid warfare: The continuation of ambiguity by other means, Eur. J. Int. Secur. 8 () 192–206, https://doi.org/10.1017/eis.2022.19.
57. NATO (2024) Energy Security, North Atlantic Treaty Organization, Brussels.
58. NATO (2026) Resilience Baseline Requirements, North Atlantic Treaty Organization, Brussels, 15 September 2026.
59. Neal AW (2026) After Nord Stream: Four security dilemmas in critical maritime infrastructure protection, Int. Aff. 102 () 207–225, https://doi.org/10.1093/ia/iiaf229.

60. Nikolopoulos D, Makropoulos C (2026) The evolution of resilience from its ecological roots to critical infrastructure applications: Concepts, definitions and future directions, Int. J. Crit. Infrastruct. Prot. 53 () 100848, https://doi.org/10.1016/j.ijcip.2026.100848.
61. Office of the President (2024) Second Meeting of the Whole-of- Society Defense Resilience Committee, Taipei, 26 December.
62. Office of the President (2026) Whole-of-Society Defense Resilience Committee: About the Committee, Taipei.
63. Ouyang M (2014) Review on modeling and simulation of interdependent critical infrastructure systems, Reliab. Eng. Syst. Saf. 121 () 43–60, https://doi.org/10.1016/j.ress.2013.06.040.
64. Pursiainen C (2018) Critical infrastructure resilience: A Nordic model in the making?, Int. J. Disaster Risk Reduct. 27 () 632–641, https://doi.org/10.1016/j.ijdrr.2017.08.006.
65. Rauta V, Monaghan S (2021) Global Britain in the grey zone: Between stagecraft and statecraft, Defence Stud. 21 () 475–497, https://doi.org/10.1080/13523260.2021.1980984.
66. Republic of China (Taiwan) (2016) Energy Administration Act, Ministry of Economic Affairs Laws and Regulations Retrieving System, Taipei, as amended 30 November.
67. Republic of China (Taiwan) (2022) Organization Act of the Administration for Cyber Security, Ministry of Digital Affairs, Taipei.
68. Republic of China (Taiwan) (2025) Special Statute on Strengthening the Resilience of the Economy, Society, and National Security in Response to International Developments, Ministry of Economic Affairs, Taipei.
69. Roege PE, Collier ZA, Mancillas J, McDonagh JA, Linkov I (2014) Metrics for energy resilience, Energy Policy 72 () 249–256, https://doi.org/10.1016/j.enpol.2014.04.012.
70. Schmitz R, Flachsbarth F, Plaga LS, Braun M, Härtel P (2025) Energy security and resilience: Revisiting concepts and advancing planning perspectives for transforming integrated energy systems, Energy Policy 207 () 114796, https://doi.org/10.1016/j.enpol.2025.114796.
71. Schreier M (2012) Qualitative Content Analysis in Practice, SAGE Publications, London.
72. Seawright J, Gerring J (2008) Case selection techniques in case study research: A menu of qualitative and quantitative options, Polit. Res. Q. 61 () 294–308, https://doi.org/10.1177/1065912907313077.
73. Taiwan Power Company (2024) Sustainability Report, Taipei, 2025. The report contains the Grid Resilience Enhancement Program and information on infrastructure impacts and recovery following the 2024 Hualien earthquake.
74. Taiwan Power Company (2026a) Building Resilient Electricity: Power Grid Resilience Enhancement Program, Taipei.
75. Taiwan Power Company (2026b) Enhancing the Green Energy Power Grid: Microgrids and Energy Storage, Taipei.

76. Taiwan Power Company (2026c) Smart Grid Development and Distributed Energy Resource Integration, Taipei.
77. Yin RK (2018) Case Study Research and Applications: Design and Methods, sixth ed., SAGE Publications, Los Angeles.
78. Younesi A, Shayeghi H, Wang Z, Siano P, Mehrizi-Sani A, Safari A (2022) Trends in modern power systems resilience: State-of-the-art review, Renew. Sustain. Energy Rev. 162 () 112397, https://doi.org/10.1016/j.rser.2022.112397.