ORIGINAL RESEARCH **Open access**

AI-Driven Energy Sovereignty: A Critical Framework for Data Ownership, Infrastructure Control, and National Energy Security

Krzysztof Wisniewski[1*], Malgorzata Nowak[1], Tomasz Adamczyk[2], Anna Kowalczyk[3]

Abstract

AI is increasingly embedded in energy systems through forecasting, optimisation, demand response, cybersecurity, market coordination, and infrastructure control. While these applications may improve efficiency and resilience, they also reshape the meaning of energy sovereignty by shifting strategic authority from physical assets alone toward data ownership, algorithmic control, cloud dependency, and platform governance. Existing energy security and sovereignty frameworks remain insufficient because they do not fully account for how AI-enabled data flows, proprietary models, foreign digital infrastructures, and opaque decision systems may create new forms of dependence and geopolitical vulnerability. This article develops a critical framework for AI-driven energy sovereignty structured around three interdependent pillars: data ownership, infrastructure control, and national energy security. Drawing on critical synthesis of energy security studies, digital sovereignty literature, AI governance, cybersecurity, and international political economy, the article argues that sovereignty in AI-enabled energy systems depends not only on who owns generation assets or grid infrastructure, but also on who controls operational data, algorithmic decision logic, model updates, cloud services, and crisis-time override capacity. The framework shows that AI-generated energy data may expose strategic vulnerabilities, external AI platforms may create hidden channels of leverage, and national energy security must be expanded to include data integrity, algorithmic autonomy, software supply-chain resilience, and protection against AI-specific threats such as data poisoning, false-data injection, model extraction, and remote algorithmic interference. The article offers analytical taxonomies of energy data risks, AI-controlled infrastructure dependencies, AI-specific security threats, and sovereignty assessment criteria. It concludes that preserving energy sovereignty in the age of AI requires proactive, multi-dimensional governance that combines data rights, infrastructure auditability, domestic failover capacity, vendor accountability, interoperability, cybersecurity assurance, and regional cooperation. The proposed framework provides a diagnostic and strategic tool for policymakers seeking to govern AI-enabled energy systems without allowing digital dependence to undermine national autonomy, resilience, or democratic control.

Keywords AI, Energy sovereignty, Data ownership, Infrastructure control, National energy security, Critical framework

*Correspondence:
Krzysztof Wisniewski
krzysztof.wisniewski@pw.edu.pl
[1] Department of Intelligent Grid Analytics and AI, Faculty of Electrical Engineering, Warsaw University of Technology, Warsaw, Poland
[2] Department of Artificial Intelligence for Energy Storage Systems, Faculty of Engineering, AGH University of Science and Technology, Krakow, Poland
[3] Department of Smart Energy Data Science, Faculty of Engineering, University of Warsaw, Warsaw, Poland

Introduction

This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), which permits non-commercial use, distribution, reproduction, and adaptation in any medium or format, provided that appropriate credit is given to the original author(s) and source, a link to the license is provided, and any changes made are indicated. Adapted material must be distributed under the same license.

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Energy sovereignty has traditionally been associated with control over fuels, generation assets, supply chains, and territorial infrastructure, yet AI-enabled digitalization is extending sovereignty struggles into data, software, cloud infrastructure, and algorithmic decision systems. Earlier discussions of energy sovereignty emphasized ownership, self-determination, and policy control over energy futures [1], while recent work shows that sovereignty also involves the ability of communities, states, and institutions to govern the terms under which energy systems are designed and operated [2]. In AI-enabled systems, this means that sovereignty cannot be reduced to who owns the grid or fuel source; it must also ask who owns operational data, who controls the algorithms, and who can intervene when automated energy decisions affect national security.

A major lacuna remains between energy sovereignty scholarship and AI governance scholarship. Energy sovereignty debates often focus on renewables, local autonomy, Indigenous energy rights, and geopolitical supply chains [3], whereas AI governance debates have concentrated on ethics, accountability, and regulatory alignment without always considering how AI infrastructures can redistribute geopolitical control [4]. This separation is problematic because cloud-hosted analytics, proprietary optimisation platforms, foreign AI vendors, and cross-border data processing may create dependencies that are less visible than fuel import dependence but potentially more difficult to reverse. AI-driven energy sovereignty therefore requires a conceptual lens that treats digital dependency as a political-economic condition, not merely a technical procurement issue.

This article argues that AI-driven energy sovereignty should be conceptualized through three interdependent pillars: data ownership, infrastructure control, and national energy security. Data ownership matters because smart meter records, grid topology information, market transactions, and operational telemetry can reveal strategic vulnerabilities and commercial patterns [5]. Infrastructure control matters because AI may be embedded in dispatch, forecasting, demand response, cybersecurity, and asset management systems that influence the real-time operation of critical infrastructure [6]. National energy security must therefore be redefined to include data integrity, algorithmic autonomy, and resilience against AI-specific coercion.

Background

Traditional energy sovereignty and its limits

Traditional energy sovereignty was grounded in the ability of states or communities to control energy resources, protect supply security, and shape development pathways according to political priorities. Castán Broto's analysis of energy sovereignty and development planning shows that sovereignty has always involved more than physical supply because it also concerns whose priorities are embedded in energy decisions [1]. Schelly, Bessette, Brosemer, Gagnon, Arola, Fiss, Pearce, and Halvorsen similarly show that policy tools can support or constrain energy sovereignty depending on whether they expand local control or reproduce dependence [2]. These insights remain valuable, but they are insufficient for AI-enabled energy systems because control can now be displaced through data platforms, software layers, and algorithmic infrastructures even when physical assets remain nationally owned.

The digital transformation of Energy Systems

The digital transformation of energy systems has embedded AI and machine learning into demand response, forecasting, optimisation, cybersecurity, market coordination, and grid management. Ahmad, Zhang, Huang, Zhang, Dai, Song, and Chen describe AI as an increasingly central element of sustainable energy systems, while Antonopoulos, Robu, Couraud, Kirli, Norbu, Kiprakis, Flynn, Elizondo-Gonzalez, and Wattam show that machine learning is already central to demand-side response architectures [6, 7]. These developments may improve operational efficiency, but they also shift authority toward actors that possess data infrastructures, model-building expertise, and computational capacity. As a result, digital transformation can create a sovereignty paradox: the more intelligent an energy system becomes, the more dependent it may become on external data-processing and algorithmic capabilities.

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Data ownership in the energy sector: a contested terrain

Energy data ownership is contested because energy data are simultaneously personal, commercial, operational, and strategic. Smart meter privacy research shows that consumption data can reveal behavioural patterns, occupancy routines, and household characteristics, making such data politically and ethically sensitive rather than merely technical [8]. Broader data sovereignty scholarship argues that control over data concerns authority, rights, accountability, and the capacity to determine how data are stored, processed, shared, and monetised [9]. In energy systems, the stakes are intensified because operational data may reveal vulnerabilities in national infrastructure, market behaviour, and grid resilience.

Infrastructure Control in an age of algorithmic management

AI enables new forms of infrastructure control by automating prediction, dispatch, anomaly detection, balancing, maintenance, and market participation. Deep-learning-based false data injection detection in smart grids illustrates the increasing reliance on intelligent mechanisms for maintaining operational security [10], while cybersecurity studies of critical energy infrastructure show that digital control systems are now central to the vulnerability landscape [11]. The problem is not only that infrastructure can be attacked digitally, but that legitimate control systems may themselves depend on foreign vendors, proprietary algorithms, or remotely maintained platforms. Infrastructure sovereignty must therefore address both hostile intrusion and ordinary dependency.

Conceptual Foundation: Redefining Energy Sovereignty

A multidimensional concept of energy sovereignty

AI-driven energy sovereignty can be conceptualized as the capacity of a political community to govern the data, algorithms, infrastructures, and institutional arrangements through which energy systems are planned, operated, secured, and transformed. Timmermann and Noboa's values-based analysis shows that energy sovereignty is not simply a material condition but a normative and political concept involving autonomy, justice, responsibility, and self-determination [3]. In AI-enabled systems, this autonomy depends on whether states and communities can determine how energy data are collected, how models are trained, how automated decisions are audited, and how critical infrastructure remains controllable under crisis conditions. Sovereignty is therefore not absolute independence but governed interdependence under conditions of accountable control.

The AI-sovereignty nexus

The AI-sovereignty nexus is ambivalent because AI may strengthen sovereignty through improved forecasting, cybersecurity, and operational coordination, while also undermining sovereignty through dependency on external platforms and opaque model infrastructures. Wang, Wang, Dong, and Nepal argue that AI can affect high-quality energy development and clean energy transitions, suggesting that AI may become strategically valuable for national energy transformation [12]. Yet digital sovereignty scholarship warns that digital infrastructures can relocate authority from public institutions to private platforms or foreign jurisdictions [13]. AI in energy should therefore be treated as both a capability and a dependency, with its sovereign value determined by who governs the data, models, standards, and infrastructure interfaces. These interdependent shifts in authority—spanning who owns energy data, who controls algorithmic infrastructure, and who retains crisis-time operational command—are visualised in **Figure 1**, which maps how states, utilities, AI vendors, cloud providers, regulators, consumers, and adversarial actors interact across AI-enabled energy systems.

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

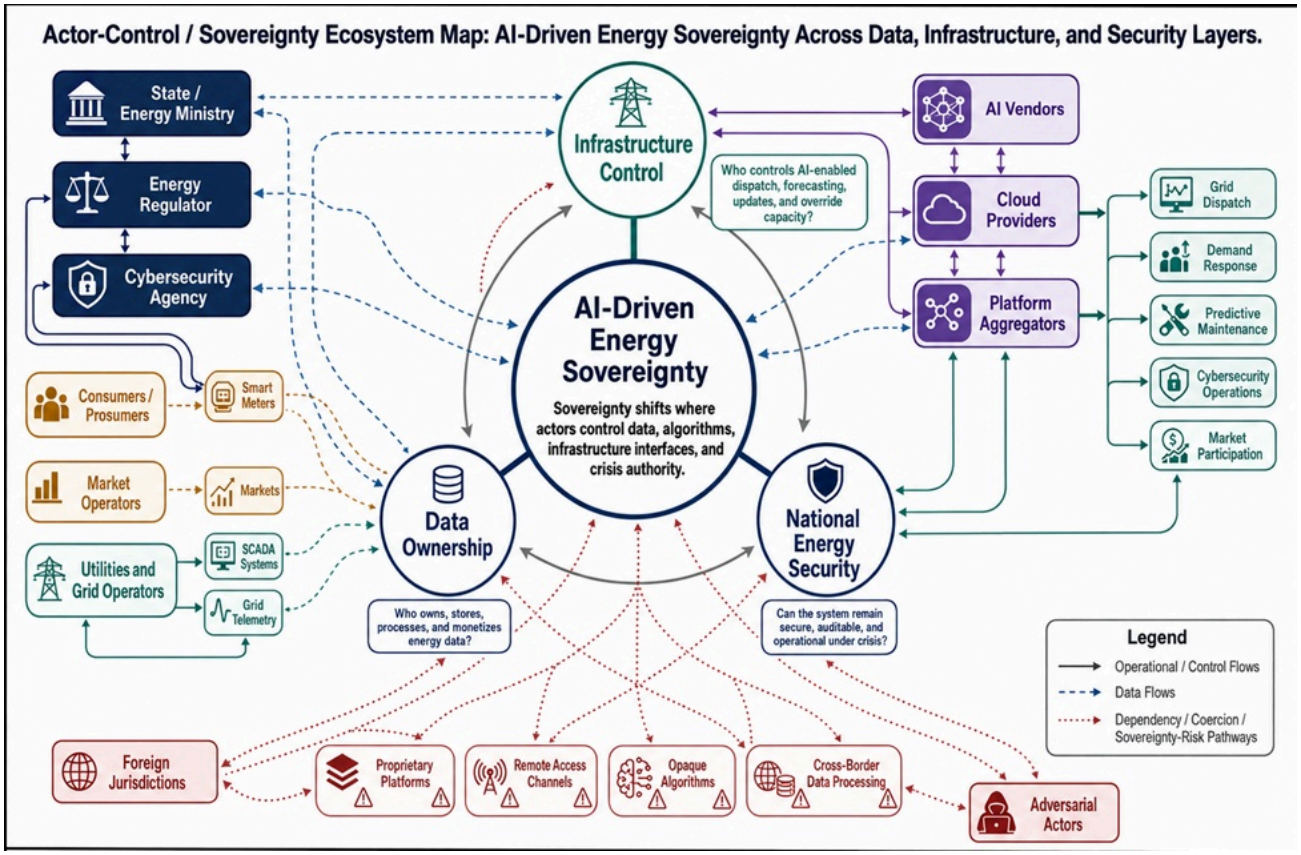

Figure 1. Actor-Control / Sovereignty Ecosystem Map: AI-Driven Energy Sovereignty across Data, Infrastructure, and Security Layers

Data Ownership and Sovereignty

Energy data types and sovereignty implications

Energy data are not homogeneous, and sovereignty risks vary according to whether data describe households, grid operations, asset conditions, generation patterns, market transactions, or security events. Smart meter data may expose personal routines and social behaviour [8], while grid operational data may reveal topology, congestion points, and critical dependencies. Data sharing in energy systems may support coordination, innovation, flexibility, and system efficiency, but it can also create asymmetrical visibility when external actors gain access to strategically valuable datasets [5]. A sovereignty framework must therefore classify energy data by sensitivity, ownership ambiguity, control risk, and cross-border exposure rather than treating all data-sharing as inherently beneficial or inherently dangerous.

Recent technical research has begun operationalising data sovereignty in energy contexts through innovative architectures combining multi-agent systems with self-sovereign identities and zero-knowledge proofs, enabling selective data disclosure that verifies information correctness without revealing underlying data [14]. This technical trajectory parallels governance-focused analyses of how generative AI applications in energy systems create novel data security risks requiring classification-based governance approaches that balance security with data sharing imperatives [15]. The convergence of technical and regulatory approaches suggests that energy data sovereignty is neither a purely technological nor purely legal problem, but rather a socio-technical governance challenge requiring coordinated innovation across both domains [16]. **Table 1** presents a taxonomy of energy data types and their associated sovereignty implications.

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Table 1. Taxonomy of Energy Data Types and Sovereignty Implications

Data Type	Source	Sensitivity Level	Sovereignty Risk	Mitigation Strategy
Generation SCADA data	Power plants, renewable farms, control systems	Very high	Reveals operational status, dispatch capacity, equipment vulnerabilities, and possible intervention points in nationally significant assets	National hosting requirements, segmented access, vendor audit rights, sovereign backup control channels
Transmission grid topology data	Transmission system operators, digital twins, network models	Very high	Enables mapping of bottlenecks, cascading-failure pathways, and strategic weak points	Classified operational-data tiering, controlled research access, encrypted domestic repositories
Distribution network telemetry	Distribution operators, sensors, substations, smart grid devices	High	Exposes local congestion, outage patterns, and dependency nodes that may be exploited during crises	Regional data trusts, strict API governance, resilience-oriented anonymisation
Smart meter personal data	Households, firms, prosumers, aggregators	High	Reveals behavioural routines, occupancy, consumption habits, and socio-economic patterns	Consumer data rights, privacy-preserving analytics, consent granularity, domestic processing for sensitive categories
Demand-response participation data	Aggregators, retailers, flexibility platforms	Medium to high	Allows external actors to infer controllable load, consumer flexibility, and emergency curtailment capacity	Licensing of aggregators, national flexibility registries, contractual restrictions on onward transfer
Market transaction data	Power exchanges, balancing markets, trading platforms	High	Reveals bidding strategies, price vulnerabilities, market concentration, and potential manipulation targets	Market surveillance access, data residency for strategic transactions, algorithmic trading disclosure
Cybersecurity event data	Security operation centres, intrusion detection systems, grid logs	Very high	Reveals attack surfaces, defensive capacity, incident response timing, and unresolved vulnerabilities	Sovereign cyber repositories, mandatory breach reporting, controlled cross-border threat intelligence
Asset maintenance and failure data	Utilities, equipment vendors, predictive maintenance platforms	Medium to high	Creates dependency on foreign vendors that may control failure forecasts and spare-part prioritisation	Data portability clauses, open maintenance logs, domestic model escrow
Weather and renewable forecasting data	Satellites, meteorological services, forecasting vendors	Medium	External forecasting dependence can affect dispatch confidence and planning autonomy	Public forecasting capacity, multi-vendor redundancy, transparent model assumptions
Energy-consumer	Apps, home energy systems, electric	Medium	Platform firms may aggregate behavioural and flexibility data	Interoperability rules, user portability rights, limits on

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

platform data	vehicle charging platforms		beyond public oversight	secondary commercial use

Cross-border data flows and dependency

Cross-border data flows can create geopolitical dependencies when energy data are stored, processed, or analysed under foreign legal regimes or by firms embedded in external strategic ecosystems. Floridi's discussion of digital sovereignty emphasizes why jurisdiction, technological dependence, and control over digital infrastructure matter especially for the European Union [17]. Couture and Toupin show that digital sovereignty is a contested concept, meaning that claims of control over data and infrastructure may differ across states, corporations, communities, and users [18]. In energy systems, this contestation becomes acute because cross-border data processing may be operationally efficient while simultaneously weakening national visibility, legal enforceability, and crisis-time autonomy.

Legal and regulatory regimes for energy data

Legal and regulatory regimes for energy data should be understood as sovereignty infrastructures because they define who may collect, transfer, process, audit, and monetize energy-related information. Hummel, Braun, Tretter, and Dabrock argue that data sovereignty involves the capacity of data subjects and institutions to control data use, while von Scherenberg, Hellmeier, and Otto show that data sovereignty also requires information-system arrangements capable of enforcing control in practice [9, 19]. Existing regimes such as privacy law, data access rules, localisation requirements, and sector-specific cybersecurity obligations may provide partial tools, but they often remain fragmented across personal data, industrial data, and critical infrastructure governance. AI-driven energy sovereignty would therefore require integrated energy data governance that distinguishes between consumer protection, operational resilience, market integrity, and national security concerns. **Table 2** presents a taxonomy of energy data types and their associated sovereignty implications, illustrating how different categories of energy-related information vary in sensitivity, exposure risks, and required governance strategies across generation, transmission, distribution, market, cybersecurity, and consumer domains.

Table 2. Taxonomy of Energy Data Types and Sovereignty Implications

Data Type	Source	Sensitivity Level	Sovereignty Risk	Mitigation Strategy
Generation SCADA data	Power plants, renewable farms, control systems	Very high	Reveals operational status, dispatch capacity, equipment vulnerabilities, and possible intervention points in nationally significant assets	National hosting requirements, segmented access, vendor audit rights, sovereign backup control channels
Transmission grid topology data	Transmission system operators, digital twins, network models	Very high	Enables mapping of bottlenecks, cascading-failure pathways, and strategic weak points	Classified operational-data tiering, controlled research access, encrypted domestic repositories
Distribution network telemetry	Distribution operators, sensors, substations, smart grid devices	High	Exposes local congestion, outage patterns, and dependency nodes that may be exploited during crises	Regional data trusts, strict API governance, resilience-oriented anonymisation

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Smart meter personal data	Households, firms, prosumers, aggregators	High	Reveals behavioural routines, occupancy, consumption habits, and socio-economic patterns	Consumer data rights, privacy-preserving analytics, consent granularity, domestic processing for sensitive categories
Demand-response participation data	Aggregators, retailers, flexibility platforms	Medium to high	Allows external actors to infer controllable load, consumer flexibility, and emergency curtailment capacity	Licensing of aggregators, national flexibility registries, contractual restrictions on onward transfer
Market transaction data	Power exchanges, balancing markets, trading platforms	High	Reveals bidding strategies, price vulnerabilities, market concentration, and potential manipulation targets	Market surveillance access, data residency for strategic transactions, algorithmic trading disclosure
Cybersecurity event data	Security operation centres, intrusion detection systems, grid logs	Very high	Reveals attack surfaces, defensive capacity, incident response timing, and unresolved vulnerabilities	Sovereign cyber repositories, mandatory breach reporting, controlled cross-border threat intelligence
Asset maintenance and failure data	Utilities, equipment vendors, predictive maintenance platforms	Medium to high	Creates dependency on foreign vendors that may control failure forecasts and spare-part prioritisation	Data portability clauses, open maintenance logs, domestic model escrow
Weather and renewable forecasting data	Satellites, meteorological services, forecasting vendors	Medium	External forecasting dependence can affect dispatch confidence and planning autonomy	Public forecasting capacity, multi-vendor redundancy, transparent model assumptions
Energy-consumer platform data	Apps, home energy systems, electric vehicle charging platforms	Medium	Platform firms may aggregate behavioural and flexibility data beyond public oversight	Interoperability rules, user portability rights, limits on secondary commercial use

Infrastructure Control and Algorithmic Autonomy

AI in critical energy infrastructure operations

AI is increasingly embedded in the operational layers of critical energy infrastructure, including SCADA analytics, energy management systems, renewable forecasting, fault detection, grid balancing, demand response, and market optimisation. Machine learning for smart grid cybersecurity demonstrates how AI can support intrusion detection, anomaly recognition, and defensive automation [20]. At the same time, the movement from human-supervised control toward algorithmically mediated operation means that infrastructure control may become dependent on model performance, vendor access, software updates, and cloud availability. Infrastructure sovereignty therefore requires attention not only to asset ownership but also to the control logic through which those assets are operated.

Foreign dependency and the risk of algorithmic leverage

Foreign dependency becomes strategically significant when AI platforms, cloud services, grid software, predictive maintenance tools, or optimisation engines are controlled by actors outside national jurisdiction. Broeders, Cristiano, and

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Kaminska show that digital sovereignty and strategic autonomy have become central to European debates because digital infrastructures are now bound up with geopolitical power [21]. In energy systems, algorithmic leverage could emerge when external providers control model updates, remote access privileges, cybersecurity patches, proprietary interfaces, or operational analytics. Such leverage does not require direct ownership of physical assets; it may arise through contractual dependency, intellectual property control, data lock-in, or the inability to substitute a critical algorithm during a crisis. **Table 3** identifies key AI-controlled infrastructure elements and their associated foreign dependency risks.

Table 3. AI-Controlled Infrastructure Elements and Foreign Dependency Risks

Infrastructure Element	AI Function	Potential Foreign Dependency	Risk Level	Autonomy Strategy
Transmission control centre	Load forecasting, congestion prediction, real-time balancing support	Proprietary optimisation engine hosted by foreign cloud provider	Very high	Domestic failover platform, mandatory audit logs, operator override, model escrow
Distribution automation systems	Fault location, outage restoration, voltage optimisation	Vendor-controlled remote diagnostics and firmware updates	High	Certified update governance, segmented access, local restoration mode
Renewable generation fleets	Forecasting, curtailment optimisation, predictive maintenance	Foreign forecasting service or turbine analytics platform	High	Multi-provider forecasting, access to raw telemetry, local maintenance models
Battery and storage assets	Charge-discharge optimisation, market participation	External aggregator controls dispatch logic and trading interface	High	Licensing of aggregators, dispatch transparency, sovereign emergency curtailment authority
Demand-response platforms	Flexible load aggregation, automated curtailment	Platform lock-in through consumer data and proprietary APIs	Medium to high	Interoperability standards, portability rights, national flexibility registry
Pipeline and fuel logistics systems	Leak detection, flow optimisation, anomaly detection	Remote analytics vendor controls monitoring models	High	Local control fallback, operational-data residency, independent model validation
Wholesale electricity markets	Algorithmic bidding surveillance, price forecasting, automated trading	Foreign trading platforms or opaque AI market agents	Very high	Algorithmic disclosure rules, market surveillance integration, limits on black-box automated bidding
Electric vehicle charging networks	Load management, dynamic pricing, vehicle-to-grid coordination	Foreign platform manages charging data and grid-response logic	Medium to high	Open charging protocols, domestic data processing, grid-operator override mechanisms
Cybersecurity operations centre	Threat detection, anomaly classification, automated response	Foreign threat intelligence or AI detection stack with opaque rules	Very high	Sovereign threat repository, explainable detection requirements, national incident response integration
Energy digital twin platforms	Simulation, scenario testing, asset modelling, control recommendations	Proprietary digital twin architecture creates	High	Open model interfaces, exportable system models,

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

		long-term knowledge dependence		public-interest digital twin governance

Strategies for preserving infrastructure autonomy

Preserving infrastructure autonomy should be addressed through a combination of technical, regulatory, procurement, and institutional strategies. Critical energy infrastructure cybersecurity literature suggests that resilience depends on anticipating evolving vulnerabilities across digital control systems rather than treating cybersecurity as an external add-on [11]. AI-specific autonomy strategies would include auditability requirements, source-code or model escrow for critical functions, domestic failover capacity, interoperability mandates, public-interest procurement standards, and emergency override authority. These strategies should not imply technological isolation, but they should ensure that interdependence remains reversible, transparent, and governable. **Table 4** highlights how increasing reliance on AI-enabled control systems across critical energy infrastructure can generate significant foreign dependency risks, underscoring the need for coordinated autonomy strategies to ensure that digital interdependence remains transparent, reversible, and governable.

Table 4. AI-Controlled Infrastructure Elements and Foreign Dependency Risks

Infrastructure Element	AI Function	Potential Foreign Dependency	Risk Level	Autonomy Strategy
Transmission control centre	Load forecasting, congestion prediction, real-time balancing support	Proprietary optimisation engine hosted by foreign cloud provider	Very high	Domestic failover platform, mandatory audit logs, operator override, model escrow
Distribution automation systems	Fault location, outage restoration, voltage optimisation	Vendor-controlled remote diagnostics and firmware updates	High	Certified update governance, segmented access, local restoration mode
Renewable generation fleets	Forecasting, curtailment optimisation, predictive maintenance	Foreign forecasting service or turbine analytics platform	High	Multi-provider forecasting, access to raw telemetry, local maintenance models
Battery and storage assets	Charge-discharge optimisation, market participation	External aggregator controls dispatch logic and trading interface	High	Licensing of aggregators, dispatch transparency, sovereign emergency curtailment authority
Demand-response platforms	Flexible load aggregation, automated curtailment	Platform lock-in through consumer data and proprietary APIs	Medium to high	Interoperability standards, portability rights, national flexibility registry
Pipeline and fuel logistics systems	Leak detection, flow optimisation, anomaly detection	Remote analytics vendor controls monitoring models	High	Local control fallback, operational-data residency, independent model validation
Wholesale electricity markets	Algorithmic bidding surveillance, price forecasting, automated trading	Foreign trading platforms or opaque AI market agents	Very high	Algorithmic disclosure rules, market surveillance integration, limits on black-box automated bidding

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Electric vehicle charging networks	Load management, dynamic pricing, vehicle-to-grid coordination	Foreign platform manages charging data and grid-response logic	Medium to high	Open charging protocols, domestic data processing, grid-operator override mechanisms
Cybersecurity operations centre	Threat detection, anomaly classification, automated response	Foreign threat intelligence or AI detection stack with opaque rules	Very high	Sovereign threat repository, explainable detection requirements, national incident response integration
Energy digital twin platforms	Simulation, scenario testing, asset modelling, control recommendations	Proprietary digital twin architecture creates long-term knowledge dependence	High	Open model interfaces, exportable system models, public-interest digital twin governance

National Energy Security Reimagined

Expanding the security perimeter

AI-driven energy sovereignty requires expanding the national energy security perimeter from physical infrastructure and fuel availability to include data integrity, algorithmic trustworthiness, software supply chains, and cloud-dependent operational continuity. The geopolitics of energy system transformation already shows that energy transitions redistribute strategic dependencies across minerals, technologies, grids, and institutions [22]. AI adds a further layer because the systems that forecast, optimise, protect, and coordinate energy flows may become decisive security assets in their own right. National energy security can therefore be framed as the capacity to maintain reliable energy services while retaining accountable control over the digital and algorithmic systems that increasingly mediate those services.

New AI-specific threats

AI-enabled energy systems face threats that differ from conventional sabotage because adversaries may manipulate the informational or algorithmic conditions under which infrastructure decisions are made. False data injection attacks demonstrate how manipulated grid data can distort situational awareness and trigger harmful operational responses if detection mechanisms fail [16]. Machine learning can also be targeted through data poisoning, model extraction, adversarial inputs, opaque vendor updates, or remote algorithmic interference, all of which may undermine energy autonomy without necessarily damaging physical assets. These threats suggest that sovereignty may be compromised not only by an external actor turning infrastructure off, but also by subtly altering how infrastructure "knows," predicts, and responds. **Table 5** presents a threat assessment framework for AI-specific energy security vulnerabilities.

Table 5. AI-Specific Energy Security Threats: A Threat Assessment Framework

Threat	Mechanism	Likelihood	Impact	Consequence	Mitigation
Data poisoning	Training or operational data are altered to distort forecasts, dispatch recommendations, or anomaly detection	Medium	High	Gradual degradation of operational judgment and unreliable automated decisions	Data provenance controls, anomaly screening, independent validation datasets
False data injection	Grid measurements are manipulated to mislead control systems or operators	Medium to high	Very high	Misallocation of generation, hidden congestion, or cascading instability	Real-time detection, redundant sensing, physics-informed validation

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Model extraction	Adversaries infer proprietary or security-relevant model behaviour through repeated queries	Medium	Medium to high	Exposure of defence logic, forecasting assumptions, or operational vulnerabilities	Query monitoring, model access controls, response obfuscation for sensitive systems
Remote algorithmic sabotage	External actor manipulates model updates, APIs, or remote service channels	Low to medium	Very high	Sudden loss of control, degraded dispatch, or compromised restoration capability	Vendor access restrictions, model escrow, offline fallback, sovereign override protocols
Platform withdrawal	Foreign provider suspends cloud, software, analytics, or maintenance services during geopolitical conflict	Medium	High	Operational disruption and loss of decision-support capacity	Domestic failover systems, multi-vendor procurement, continuity clauses
Algorithmic market manipulation	AI trading agents exploit price signals, congestion patterns, or regulatory blind spots	Medium	High	Volatility amplification, unfair market outcomes, and loss of public trust	Market surveillance AI, algorithmic disclosure, trading constraints
Cybersecurity model evasion	Attackers design inputs to bypass AI-based threat detection systems	Medium	High	Undetected intrusion or delayed incident response	Human-in-the-loop review, adversarial testing, diverse detection models
Strategic energy-data exfiltration	Sensitive operational, consumer, or market datasets are transferred to external actors	Medium	High	Loss of strategic secrecy and enhanced adversary targeting capacity	Data residency, encryption, access audits, national data classification

Reconceptualizing energy security frameworks

An AI-augmented energy security framework should integrate traditional concerns with availability, affordability, reliability, and resilience alongside newer concerns with data control, algorithmic accountability, platform dependency, and geopolitical exposure. Research on renewable energy geopolitics shows that the transition to cleaner systems does not eliminate geopolitical competition but reconfigures it around new technologies, supply chains, and infrastructures [23]. Similarly, AI does not remove energy security risks; it relocates them into data pipelines, software architectures, model governance, and cross-border service dependencies. The framework proposed here therefore treats AI-specific threats as inseparable from national energy security rather than as secondary cybersecurity issues.

Resilience and response in AI-enabled energy systems

Resilience in AI-enabled energy systems should move from reactive recovery toward anticipatory, adaptive, and politically accountable response capacity. Cybersecurity research on smart grids indicates that machine learning can improve detection and response, but it also shows that defensive systems themselves become part of the security architecture that must be protected [20]. AI-enabled resilience should therefore include model monitoring, secure data governance, fallback control modes, human expertise preservation, and transparent escalation procedures. Energy sovereignty is

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

strengthened when AI supports resilience without making the system dependent on a single opaque vendor, platform, or jurisdiction.

Governance and Policy Implications

National strategies for AI-energy sovereignty

National strategies for AI-energy sovereignty should combine digital industrial policy, critical infrastructure regulation, data governance, AI assurance, and energy security planning. The Chinese approach to AI policy, ethics, and regulation illustrates how states may integrate AI governance with broader strategic and institutional priorities [24], while techno-nationalism scholarship cautions that nationalist technology strategies can produce illusions of control if they underestimate interdependence and global innovation networks [25]. A balanced sovereignty strategy should therefore avoid both uncritical dependence and unrealistic autarky. It should focus on strategic autonomy through domestic capacity, trusted partnerships, enforceable procurement standards, public-interest data governance, and resilience against coercive dependencies.

Multilateral and regional cooperation

AI-driven energy sovereignty also requires multilateral and regional cooperation because energy systems, data flows, technology markets, and cyber threats do not stop at national borders. Comparative work on regional energy data governance in ASEAN and the EU shows that data governance is increasingly embedded in the geopolitics of energy transition and regional cooperation [26]. Regional digital sovereignty debates further suggest that cooperation can strengthen autonomy when states coordinate standards, data spaces, certification systems, and infrastructure safeguards [21]. The policy challenge is to build cooperation that enables trusted data exchange and technological interoperability without reproducing dependence on dominant platforms or excluding less powerful states from AI-energy governance.

Evaluation Strategy for the Sovereignty Framework

Conceptual coherence and critical depth

The framework can be evaluated conceptually by asking whether it coherently connects energy sovereignty, digital sovereignty, infrastructure control, and national security without collapsing them into a single concept. Energy sovereignty scholarship emphasizes autonomy, values, and control [3], while digital sovereignty literature highlights jurisdiction, technological authority, and contested governance over digital infrastructures [13]. The framework's critical depth lies in treating AI not as a neutral efficiency tool but as a political-economic infrastructure that may redistribute power among states, corporations, communities, and technology providers. Its coherence should therefore be judged by how well it explains the interdependence of data ownership, infrastructure control, and security consequences.

Relevance to policy and strategic decision-making

The framework is relevant to policy because it translates abstract sovereignty concerns into governance questions about data access, vendor dependency, algorithmic auditability, and crisis-time operational control. Research on energy-producing Native Nations shows that sovereignty-oriented energy policy must address institutional barriers, ownership structures, and capacity constraints rather than assuming that formal authority automatically produces control [27, 28]. The same logic applies at national scale: formal ownership of infrastructure may mean little if AI systems, operational data, and software dependencies are controlled elsewhere. Policymakers could use the framework to evaluate procurement, data governance, infrastructure regulation, cybersecurity planning, and strategic partnerships.

Transferability across regions and system types

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

The framework is transferable across regions and system types because it does not assume a single energy mix, political regime, or technological pathway. Renewable energy geopolitics shows that different countries experience energy transition dependencies in different ways depending on resources, technologies, institutions, and international position [23, 29]. Similarly, AI-driven sovereignty risks will vary between highly digitalized grids, emerging energy systems, island grids, regional power pools, and countries dependent on imported digital infrastructure. The framework should therefore be applied contextually, with attention to regional capacity, legal regimes, market structures, and geopolitical exposure.

Limitations

Conceptual nature and the need for empirical testing

This article is conceptual and does not test the framework through operational data, case studies, interviews, incident analysis, or comparative policy evaluation. As AI applications in sustainable energy and demand-side response continue to expand, empirical research will be needed to determine how platform dependency, data governance, and infrastructure autonomy operate in specific energy contexts [6, 7]. The tables proposed here should therefore be read as analytical tools rather than validated measurement instruments. Future work should assess whether the categories capture real-world institutional risks and whether additional dimensions, such as financial sovereignty or mineral supply-chain sovereignty, should be integrated.

Rapid geopolitical and technological change

A second limitation is that AI-energy sovereignty is evolving rapidly as cloud architectures, AI regulation, cybersecurity threats, and geopolitical alignments change. Digital sovereignty debates show that the meaning of sovereignty in digital contexts remains contested and historically contingent [17, 18]. Energy systems are also undergoing transformation through renewables, electrification, decentralisation, and data-intensive coordination, making dependency patterns unstable over time [22]. The framework should therefore be periodically revised as new AI capabilities, governance models, and geopolitical conflicts reshape the conditions under which energy sovereignty can be protected.

Conclusion

AI-driven energy sovereignty requires a tripartite redefinition of sovereignty around data ownership, infrastructure control, and national energy security. This article has argued that sovereignty in AI-enabled energy systems cannot be understood through physical assets alone. It must also account for who controls data, who governs algorithms, and who can maintain operational authority under geopolitical stress.

The urgency of this redefinition lies in the growing dependence of energy systems on digital platforms, cloud services, automated decision systems, and cross-border data flows. These dependencies may improve efficiency and resilience under ordinary conditions, but they may also create hidden channels of coercion, lock-in, and strategic vulnerability. Energy sovereignty therefore requires proactive governance before dependency becomes structurally irreversible.

Future research should bring together energy policy, AI governance, cybersecurity, international political economy, law, and critical infrastructure studies. Policymakers should treat AI-driven energy sovereignty as a strategic governance challenge rather than a narrow technical matter. International dialogue will also be essential, because sovereign control over AI-enabled energy systems must be pursued without fragmenting the cooperation needed for secure, sustainable, and equitable energy transitions.

Acknowledgements

None

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 12 Sep 2023 Revised: 18 Nov 2023 Accepted: 05 Dec 2023
Published online: 15 June 2025

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at https://creativecommons.org/licenses/by-nc-sa/4.0/.

References

1. Castán Broto V. Energy sovereignty and development planning: the case of Maputo, Mozambique. Int Dev Plan Rev. 2017;39(3):229-48. https://doi.org/10.3828/idpr.2017.9.

2. Schelly C, Bessette D, Brosemer K, Gagnon VS, Arola KL, Fiss A, et al. Energy policy for energy sovereignty: Can policy tools enhance energy sovereignty? Sol Energy. 2020;205:109-12. https://doi.org/10.1016/j.solener.2020.05.056.

3. Timmermann C, Noboa E. Energy sovereignty: a values-based conceptual analysis. Sci Eng Ethics. 2022;28(6):54. https://doi.org/10.1007/s11948-022-00409-x.

4. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. Nat Mach Intell. 2019;1(9):389-99. https://doi.org/10.1038/s42256-019-0088-2.

5. Wang J, Gao F, Zhou Y, Guo Q, Tan CW, Song J, et al. Data sharing in energy systems. Adv Appl Energy. 2023;10:100132. https://doi.org/10.1016/j.adapen.2023.100132.

6. Ahmad T, Zhang D, Huang C, Zhang H, Dai N, Song Y, et al. Artificial intelligence in sustainable energy industry: status quo, challenges and opportunities. J Clean Prod. 2021;289:125834. https://doi.org/10.1016/j.jclepro.2021.125834.

7. Antonopoulos I, Robu V, Couraud B, Kirli D, Norbu S, Kiprakis A, et al. Artificial intelligence and machine learning approaches to energy demand-side response: a systematic review. Renew Sustain Energy Rev. 2020;130:109899. https://doi.org/10.1016/j.rser.2020.109899.

8. Asghar MR, Dán G, Miorandi D, Chlamtac I. Smart meter data privacy: a survey. IEEE Commun Surv Tutor. 2017;19(4):2820-35. https://doi.org/10.1109/COMST.2017.2693246.

9. Hummel P, Braun M, Tretter M, Dabrock P. Data sovereignty: a review. Big Data Soc. 2021;8(1):2053951720982012. https://doi.org/10.1177/2053951720982012.

10. He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans Smart Grid. 2017;8(5):2505-16. https://doi.org/10.1109/TSG.2017.2666246.

11. Sanders P, Bronk C, Bazilian MD. Critical energy infrastructure and the evolution of cybersecurity. Electr J. 2022;35(10):107224.

12. Wang B, Wang J, Dong K, Nepal R. How does artificial intelligence affect high-quality energy development? Achieving a clean energy transition society. Energy Policy. 2024;186:114010. https://doi.org/10.1016/j.enpol.2024.114010.

13. Pohle J, Thiel T. Digital sovereignty. Internet Policy Rev. 2020;9(4). https://doi.org/10.14763/2020.4.1532.

14. Heess P, Holly S, Körner MF, Nieße A, Radtke M, Schick L, et al. A multi-agent approach with verifiable and data-sovereign information flows for decentralizing redispatch in distributed energy systems. Energy Inform. 2025;8(1):24. https://doi.org/10.1186/s42162-024-00464-7.

15. Vamvakas D, Papaioannou I, Tsaknakis C, Sgouros T, Korkas C. Generative AI for sustainable smart environments: a review of energy systems, buildings, and user-centric decision-making. Energies. 2025;18(23):6163. https://doi.org/10.3390/en18236163.

16. Durmus Senyapar HN, Bayindir R. The energy hunger paradox of artificial intelligence: end of clean energy or magic wand for sustainability? Sustainability. 2025;17(7):2887. https://doi.org/10.3390/su17072887.

17. Floridi L. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. Philos Technol. 2020;33(3):369-78. https://doi.org/10.1007/s13347-020-00423-6.

18. Couture S, Toupin S. What does the notion of "sovereignty" mean when referring to the digital? New Media Soc. 2019;21(10):2305-22. https://doi.org/10.1177/1461444819865984.

19. von Scherenberg F, Hellmeier M, Otto B. Data sovereignty in information systems. Electron Mark. 2024;34(1):15. https://doi.org/10.1007/s12525-024-00693-4.

20. Berghout T, Benbouzid M, Muyeen SM. Machine learning for cybersecurity in smart grids: a comprehensive review-based study on methods, solutions, and prospects. Int J Crit Infrastruct Prot. 2022;38:100547. https://doi.org/10.1016/j.ijcip.2022.100547.

21. Broeders D, Cristiano F, Kaminska M. In search of digital sovereignty and strategic autonomy: normative power Europe to the test of its geopolitical ambitions. J Common Mark Stud. 2023;61(5):1261-80.

22. Blondeel M, Bradshaw MJ, Bridge G, Kuzemko C. The geopolitics of energy system transformation: a review. Geogr Compass. 2021;15(7):e12580. https://doi.org/10.1111/gec3.12580.

23. Vakulchuk R, Overland I, Scholten D. Renewable energy and geopolitics: a review. Renew Sustain Energy Rev. 2020;122:109547.

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press

https://doi.org/10.1016/j.rser.2019.109547.

24. Roberts H, Cowls J, Morley J, Taddeo M, Wang V, Floridi L. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. In: Ethics, governance, and policies in artificial intelligence. Cham: Springer International Publishing; 2021. p.47-79.

25. Luo Y. Illusions of techno-nationalism. J Int Bus Stud. 2022;53(3):550.

26. Yu K, Sung J, Zhou Y. Data governance in the geopolitics of energy transition: comparing regional energy cooperation in ASEAN and the EU. Politics Gov. 2025;13:10429. https://doi.org/10.17645/pag.10429.

27. Lee D, Schelly C, Gagnon VS, Smith S, Tiwari S. Preferences and perceived barriers to pursuing energy sovereignty and renewable energy: a tribal nations perspective. Energy Res Soc Sci. 2023;97:102967. https://doi.org/10.1016/j.erss.2023.102967.

28. Raimi D, Davicino A. Securing energy sovereignty: a review of key barriers and opportunities for energy-producing Native nations in the United States. Energy Res Soc Sci. 2024;107:103324. https://doi.org/10.1016/j.erss.2023.103324.

29. Overland I. The geopolitics of renewable energy: debunking four emerging myths. Energy Res Soc Sci. 2019;49:36-40. https://doi.org/10.1016/j.erss.2018.10.018.

© 2025 The Author(s). | Published by Institute of Smart Energy Systems Press