OPEN ACCESS

Smart Grids ARTICLE

The Innovation Energy

Enhancing cyber resilience of high-renewable power systems: Threat pathways and targeted countermeasures

Yifan Liu,[1] Mengxiang Liu,[1] Wenxuan Ma,[1] Ruilong Deng,[1,*] Peng Cheng,[1] and Jiming Chen[1]

*Correspondence: dengruilong@zju.edu.cn

Received: January 15, 2026; Accepted: May 29, 2026; Published Online: July 18, 2026; https://doi.org/10.59717/j.xinn-energy.2026.100169

GRAPHICAL ABSTRACT

PUBLIC SUMMARY

- High penetration of Renewable Generation Units (RGUs) with Internet of Things (IoT) expands power grid cyberthreats, requiring targeted defense research on attack impact mechanisms.
- The MRGIoT (Manipulation of Renewable Generation via IoT botnet) framework is proposed to assess grid-disruption risks of RGUs by manipulating active power using grid topology and load density data.
- Simulations on Texas grid and New Zealand North Island power system (NIPS) prove high-degree, high-load-area RGUs cause severe power loss in peak hours, while small-capacity RGUs (≤20 MW in Texas, ≤4 MW in NIPS) have negligible system risks.
- These findings provide clear and actionable guidance for strengthening the security and resilience of future net-zero power systems, supporting security planning for high-renewable zero-carbon grids.

ARTICLE Smart Grids

www.the-innovation.org/the-innovation-energy

Enhancing cyber resilience of high-renewable power systems: Threat pathways and targeted countermeasures

Yifan Liu,[1] Mengxiang Liu,[1] Wenxuan Ma,[1] Ruilong Deng,[1,*] Peng Cheng,[1] and Jiming Chen[1]

[1]State Key Laboratory of Industrial Control Technology and College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China

*Correspondence: dengruilong@zju.edu.cn

Received: January 15, 2026; Accepted: May 29, 2026; Published Online: July 18, 2026; https://doi.org/10.59717/j.xinn-energy.2026.100169

Citation: Liu Y., Liu M., Ma W., et al. (2026). Enhancing cyber resilience of high-renewable power systems: Threat pathways and targeted countermeasures. *The Innovation Energy* **3**:100169.

High integration of Renewable Generation Units (RGUs), such as photovoltaic panels and wind turbines, is transforming modern power systems while also creating new cyber-attack surfaces due to the widespread adoption of Internet of Things (IoT) technologies. Understanding this emerging threat and its underlying impact mechanisms is essential for developing effective cyber-defense methods. This study presents MRGIoT (Manipulation of Renewable Generation via IoT botnet), a framework designed to evaluate which RGUs are most significant to the supply-demand balance and potentially capable of causing grid disruption. The framework focuses on the manipulation of RGU active power and leverages publicly available topology and operational data to identify high-value targets based on node degree and regional load density. Extensive simulations on the Texas grid model and the North Island power system (NIPS) of New Zealand show that RGUs located at high-degree nodes or in regions with high load density can trigger notable demand loss, especially during peak-load periods. These areas therefore represent priority targets for security reinforcement, infrastructure concealment, and operational safeguards. In contrast, RGUs with active power generation below certain thresholds, specifically 20 MW on the Texas model and 4 MW on the NIPS, exhibit limited system-scale impact even when placed at highly vulnerable grid locations. As renewable penetration rises and IoT adoption deepens, these findings provide clear and actionable guidance for strengthening the security and resilience of future net-zero power systems.

INTRODUCTION

The global power system is undergoing a transformative shift as the integration of inverter-based resources continues to grow.[1] Renewable Generation Units (RGUs) such as Photovoltaic (PV) panels and Wind Turbines (WTs) generation have emerged as dominant contributors to the energy mix, reshaping the landscape of electricity production worldwide.[2] The Solar Energy Industries Association forecasts that over 100 million households will have PV systems by 2030.[3] In parallel, wind power has experienced substantial growth, particularly in Europe, where Denmark leads with 57.7% of its electricity generated from WTs. In the first half of 2024, renewable energy accounted for more than 50% of total power generation across Europe, marking a significant milestone in the region's transition toward net-zero power systems.

The intermittent and decentralized nature of RGUs poses significant challenges to grid stability and real-time visibility, which cannot be adequately addressed by conventional grid infrastructure. To overcome these challenges, a wide array of Internet of Things (IoT) enabled devices must be deployed into the grid, such as smart meters, intelligent sensors, IoT gateways, edge controllers, remote terminal units (RTUs), and smart protection relays. These inherently digital and communication-enabled IoT devices form an extensive network of sensors, controllers, and interfaces, which streamlines monitoring and maintenance while introducing numerous attack surfaces that are largely absent in conventional synchronous generation facilities. Publicly disclosed vulnerabilities associated with IoT-connected RGUs have shown a persistent upward trend over time (Figure 1A). Major cyber incidents have followed a similar upward trajectory, with attacks becoming more frequent and sophisticated over time. Early events represented exploratory intrusions in industrial environments, whereas later ones reflect more coordinated, targeted, and often state-linked campaigns against power infrastructure[4] (Figure 1B). Beyond these cyber threats, the large-scale integration of RGUs itself weakens system strength. Unlike conventional synchronous generators, RGUs rely on power electronic converters with negligible inertia and weak voltage support. As RGU penetration increases, the same amount of manipulated renewable power induces larger frequency deviations and forced load shedding (Figure 1C). Together, these observations reveal a growing fragility in power systems as digital interconnection deepens and renewable integration accelerates, where cyber vulnerabilities can be directly translated into physical disruptions[55] that escalate with the growing integration of IoT-enabled RGUs.

Despite the growing risks outlined above, existing research on renewable generation security has focused primarily on physical vulnerabilities or conventional cyber threats such as data integrity attacks. Little attention has been paid to the systemic risk posed by large-scale, coordinated manipulation of distributed RGUs via IoT botnets. In particular, IoT botnets have demonstrated the ability to infiltrate hundreds of thousands of IoT-connected devices,[56–60] and their architecture can be readily adapted to target renewable assets such as residential, commercial, and utility-scale PV installations, as well as WTs across all scales. Compromised RGUs could be precisely orchestrated in a coordinated way, enabling adversaries to introduce power disturbances large enough to disrupt grid stability. This risk is amplified by the uniformity of communication protocols and software platforms across many renewable assets, which increases the likelihood that a single infection vector could propagate widely and rapidly. However, no existing framework systematically evaluates which renewable units, and under what conditions, would pose the greatest threat to grid stability based on network topology and operational characteristics. Motivated by this gap, this study aims to develop a framework to evaluate the impact of IoT-enabled manipulation of RGUs on renewable-dominated power systems and to identify the structural and operational characteristics that determine RGU's criticality to the supply-demand balance.

To achieve these objectives, we introduce MRGIoT (Manipulation of Renewable Generation via IoT botnet), a framework that links cyber-attack strategies with power system topology and operational characteristics, providing a concrete realization of how cyber-layer vulnerabilities can be exploited to induce system-level reliability degradation. The framework is developed and validated using the Texas grid model and the North Island power system (NIPS) model of New Zealand. The main contributions of this work are threefold. First, we identify two structural and operational characteristics that amplify attack effectiveness, namely high-degree network nodes and regions with elevated load density during peak-load periods. Second, these insights establish clear priorities for defensive planning including targeted protection of structurally critical nodes, enhanced obscuration of sensitive infrastructure, and robust cyber security hardening for IoT-connected renewable assets. Third, the MRGIoT framework provides a systematic tool for assessing the vulnerability of modern power systems under coordinated IoT botnet attacks. As renewable integration accelerates and IoT integration becomes ubiquitous, ensuring the resilience of future power systems is a pressing global imperative. This study aims to provide a rigorous foundation for assessing emerging vulnerabilities and outlines actionable directions for reinforcing the security of future net-zero energy systems.

MATERIALS AND METHODS

Power grid model of Texas

In this study, we adjust the temporal profiles of both generation and load in

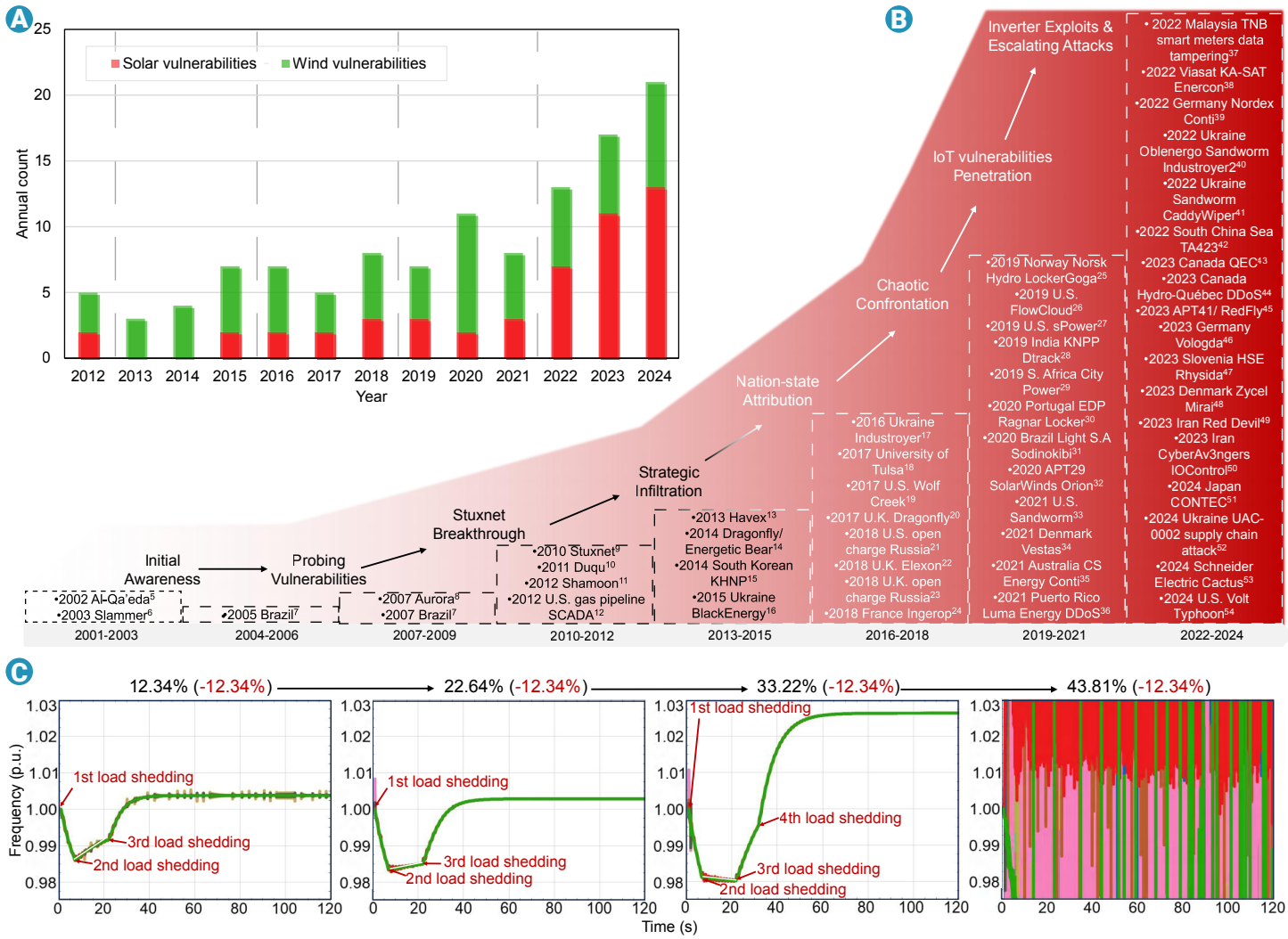

Figure 1. Escalating cyber security posture of power systems dominated by RGUs (A) The number of publicly disclosed cyber vulnerabilities affecting RGUs has steadily increased from 2012 to 2024. (B) A chronological overview of major cyber security incidents since 2003 highlights an evolution in attack sophistication and intent.[5–54] Early incidents primarily involved probing and experimental intrusions within industrial operation environments. These were followed by more deliberate and state-sponsored disruption attempts. Most recently, cyber-attacks have become more frequent and sophisticated, specifically targeting renewable energy infrastructure such as smart inverters, coinciding with the widespread adoption of IoT technologies therein. (C) The frequency fluctuation and triggered load shedding under RGU manipulation attacks in the modified IEEE 39-bus model as the increase of renewable integration. The value above each figure indicates the proportion of active power generated by RGUs, while the value in parentheses represents the proportion of active power manipulated by the adversary. This example underscores the intensifying vulnerability of power systems as the level of RGU integration continues to rise.

the Texas grid model to reflect real-world operating conditions. Solar and wind generation outputs are computed from ERCOT's 2023 hourly data, yielding six representative time points (4 am, 8 am, noon, 4 pm, 8 pm, and midnight) for four characteristic months (February, May, August, and November) for a total of twenty-four sampling points. All other generator profiles are taken directly from the model's original data, while nuclear output remains fixed (see the Data Availability).

Load profiles are updated using ERCOT's 2023 consumption data for the eight weather regions. For each region i and sampling time j, we first compute the consumption ratio

$$f_{ij} = \frac{L_{ij}}{L_i}$$

where L_{ij} denotes the active power supplied by region i at time j, L_i represents the installed generation capacity of region i. We then derive an adjusted scaling factor

$$F_{ij} = f_{ij} \cdot \left(1 - \frac{C_j + c}{LZ_i}\right)$$

where C_j is the gap between actual system consumption and total generation at time j, c is the discrepancy between the model's total generation and ERCOT's reported 2023 generation, L is Texas's total annual load and Z_i is the ratio of consumption to L at time j. This adjustment ensures that subsequent power-flow analyses remain physically consistent and numerically valid. Detailed modification curves for both generation and load are provided in Supplemental Note 4.

Quantitative metrics for RGU target selection

Identifying critical nodes is central to the MRGIoT framework. To this end, we evaluated two topology-based metrics: degree centrality and semi-local centrality,[105] alongside three metrics derived from operational conditions: the generation-to-load ratio, load density and load variability. The active power output of individual generation units is incorporated as an additional screening criterion, while demand loss is used as the primary measure for quantifying attack effectiveness.

In our framework, a node comprises a high-voltage bus and its connected low-voltage buses. Each node therefore has a degree centrality and a semi-local centrality value. At any sampling time, each grid region is characterized by its generation-to-load ratio, load density and load variability. Extensive experiments revealed no clear relationship between semi-local centrality or load variability and demand loss. Degree centrality and load density, by contrast, showed a strong positive correlation with demand loss, while gener-

ation-to-load ratios proved unreliable due to inter-regional power flows (Supplemental Note 2). Therefore, we adopted node degree, defined as the number of first-order neighbors of a node and reflecting the essence of degree centrality, along with load density to identify high-impact targets. Load density is calculated as

$$\rho_{ij} = \frac{L_{ij}}{A_i}$$

where A_i is the geographic area of region i.

Dynamic load modeling

This study adopts the constant power and constant current models from the ZIP load model (ZIP-LM). Within the DIgSILENT PowerFactory,[87] these models are categorized as nonlinear voltage-dependent and linear frequency-dependent models. The active power is computed as:

$$P = P_0 \cdot \left[aP \cdot \left(\frac{|\underline{u}|}{|\underline{u_{ini}}|} \right)^{e\_aP} + bP \cdot \left(\frac{|\underline{u}|}{|\underline{u_{ini}}|} \right)^{e\_bP} + cP \cdot \left(\frac{|\underline{u}|}{|\underline{u_{ini}}|} \right)^{e\_cP} \right] \cdot (1 + kpf \cdot \Delta f),$$

$$\Delta f = f_e - 1 = F_e / F_{nom} - 1,$$

$$cP = 1 - aP - bP.$$

Here, P_0 is the active power of the load under normal conditions, and $|\underline{u_{ini}}|$ is the voltage at the load bus under normal conditions. P and $|\underline{u}|$ represent the active power and voltage at the load bus under current conditions, respectively. The term Δf captures the deviation of system frequency from the nominal frequency. All other terms denote model parameters.

In the IEEE 39-bus model, all loads are modeled as constant-power components. Under-frequency load shedding (UFLS) is enabled to evaluate the system's response to disturbances.[106] The load model parameters are specified as: $aP = 1$, $bP = 0$, $e\_aP = 0$, and $kpf = 0$. Under this parameterization, the dynamic load model simplifies to

$$P = P_0$$

For the Texas grid model and the North Island power system model of New Zealand, all loads are set as constant-current with $aP = 0$, $bP = 1$, and $kpf = 0$, which gives

$$P = P_0 \cdot \frac{|\underline{u}|}{|\underline{u_{ini}}|}$$

UFLS protection is not implemented in this model. The active power of each load dynamically responds to change in its local bus voltage. The impact of disturbances is quantified by computing total demand loss, defined as the cumulative deviation in active power consumption. Notably, if the voltage at certain load buses increases following an attack, their power consumption may also increase, potentially leading to a negative net reduction in total demand. Furthermore, the presence of conventional generators, besides wind and solar units, in both the Texas and the North Island power system models allows for compensatory responses. During an attack, some generators increase their output to compensate, which can result in a negative demand loss.

Construction of a renewable-dominated IEEE 39-bus test system

The IEEE 39-bus system is selected as the initial test system for four reasons. First, as an official IEEE standard, it provides a well-validated baseline for reproducibility. Second, its transmission-level topology is appropriate for analyzing utility-scale renewable generation units connected directly to the transmission grid. Third, its moderate scale of 10 generators and 39 buses accommodate the extensive combinatorial experiments required in the exploratory phase, whereas a smaller system lacks sufficient topological complexity and a larger system such as the Texas 2000-bus model is less suitable for initial validation. Fourth, this system enabled a key insight that generators must exceed a power threshold before node degree becomes a meaningful vulnerability metric. This insight directly informed the subsequent analysis on the Texas 2000-bus model. This stepwise approach from a controlled test system to a large-scale practical model ensures that the conclusions are both mechanistically grounded and practically relevant.

We outline the procedure for transforming the IEEE 39-bus system[107] into a testcase with high renewable penetration level. To assess the system's voltage stability under different generator configurations, the VQ curve is used. The objective is to replace as many conventional synchronous generators as possible with RGUs, while maintaining the critical point of the VQ curve at a voltage and reactive power level as low as possible. In the modified model, bus 39 remains connected to the external grid and bus 31 continues to serve as the slack bus. Generators at buses 30, 32, 33, 34, 35, 36, 37, and 38 are sequentially replaced with RGUs, and the resulting impact on the VQ curve at bus 39 is assessed. This replacement progressively weakens the system's voltage-support capability. When fewer than five buses are converted, corresponding to a renewable penetration below 43.81%, the VQ curve at bus 39 remains largely unchanged. Accordingly, generators at buses 30, 32, 33, 34, and 35 are selected for conversion to renewable units (see Supplemental Note 3 for details).

Because PVs provide limited reactive power, we set their local control mode to const_Q, while WTs, supported by mechanical inertia, are set to const_V. The same settings are applied in the modified Texas grid model (see Supplemental Note 6 for details). However, on the NIPS model, both PVs and WTs are set to const_Q mode,[108] and we kept this setting unchanged.

Under-frequency load shedding configuration

In the IEEE 39-bus model, all loads are configured as constant power loads, and under-frequency load shedding (UFLS) protection is implemented via relays on four specific loads. The nominal system frequency is 60.00 Hz. Shedding thresholds are set at 59.80 Hz, 59.50 Hz, 59.00 Hz, and 58.00 Hz, and are assigned to loads 16, 21, 23, and 15, respectively.[106] Each load is associated with a distinct delay time before disconnection: 0.01 seconds for load 16, 5.00 seconds for load 21, 20.00 seconds for load 23, and 30.00 seconds for load 15. As a result, in Figure 1C, load 16 is the first to be shed, followed by loads 21, 23, and 15 in that order. As the share of renewable generation increases further, the system becomes unstable and collapses completely.

RESULTS

MRGIoT Framework

The MRGIoT framework formalizes the end-to-end process through which an adversary identifies high-value RGU targets using publicly accessible information and executes coordinated IoT-botnet-enabled manipulations based on established exploitation techniques. As illustrated in Figure 2, the framework consists of four integrated components that together characterize how reconnaissance of network structure and operational conditions can inform the selection of strategically influential RGUs. This selection process enables coherent botnet deployment aiming to manipulate active power injections. Consistent with established threat modeling practices, we assume that the adversary has already completed the necessary phases of the information technology and operational technology intrusion phases, including reconnaissance, exploitation, privilege escalation, and lateral movement,[61] thereby possessing both access to critical physical system information and the capability to manipulate RGU power injections.

One-time power system topology data acquisition stage

The power grid can be abstracted as nodes and their interconnections, forming a complex network.[65] Prior research has shown that the topology of such systems is essential for vulnerability assessment, as centrality measures can identify nodes that are more likely to trigger cascading failures during disruptions.[66–68] Research[69] indicates that publicly accessible data sources can be leveraged to infer grid configuration and topology. Since transmission lines and substations are typically located overground, they can be identified using online geospatial mapping tools such as Google Maps.[62] Furthermore, open-source infrastructure datasets, such as those available from the Open Infrastructure Map,[63] provide geospatial data for over 5.5 million kilometers of power lines, 1 million substations, and 100,000 power plants, covering a substantial portion of the global electricity transmission

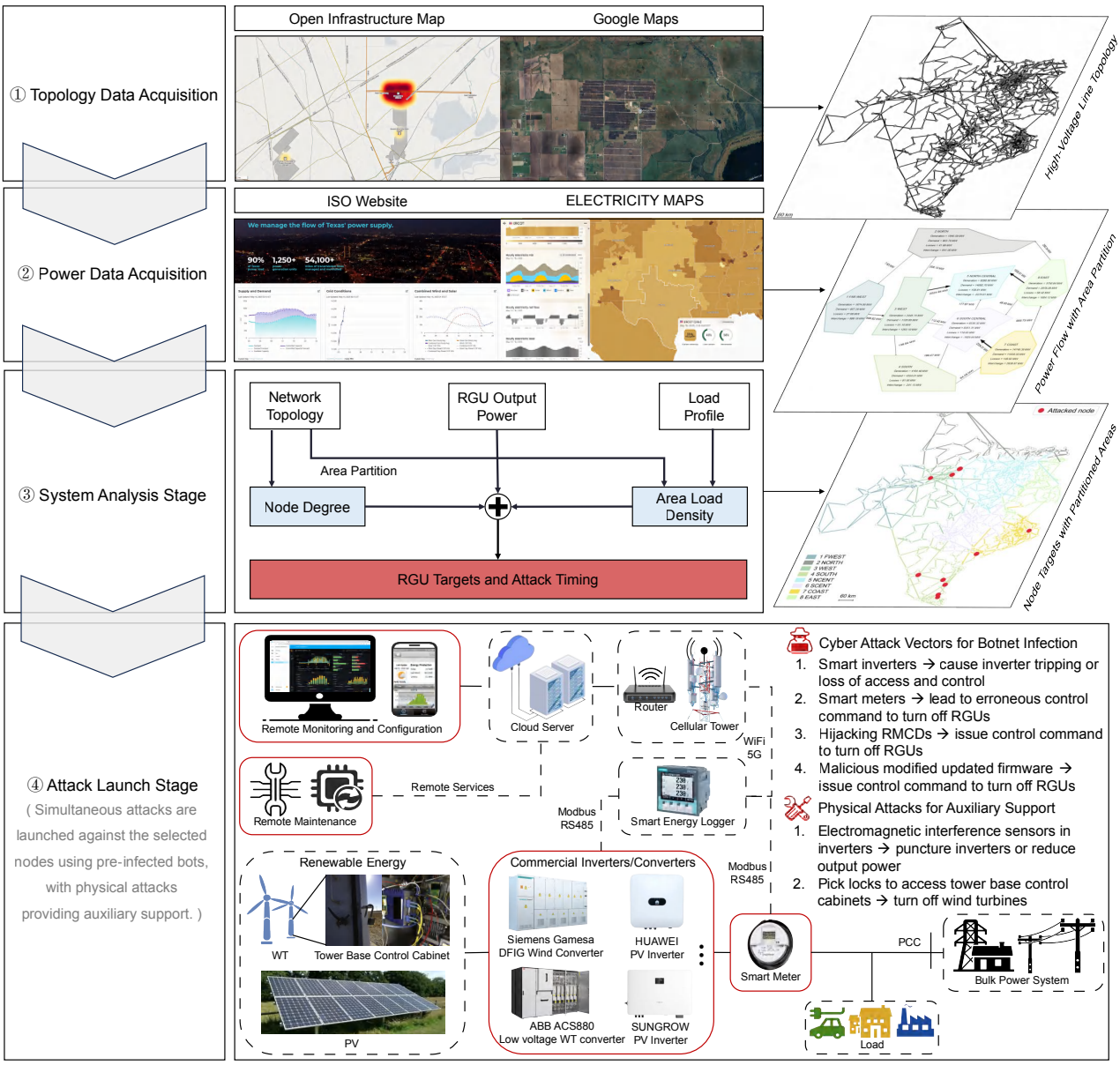

Figure 2. Overview of the MRGIoT framework ① Topology Data Acquisition: the attacker acquires the power grid topology using tools such as Google Maps[62] and Open Infrastructure Map.[63] This process is typically performed once, as the grid topology remains stable over a long period; ② Power Data Acquisition: the attacker collects power supply and demand data from various regions within the target grid by scraping public resources such as ISO Website and ELECTRICITY MAPS;[64] ③ System Analysis Stage: the attacker analyzes the collected network topology and load profile to calculate the node degree and area load density, with which the RGU targets and attack timing are identified considering the output powers of RGUs; ④ Attack Launch Stage: the attacker utilizes the IoT-connected RGUs botnet to manipulate identified RGU targets at a predetermined time. The detailed botnet propagation process can be referenced from the Mirai botnet.[56] Corresponding to steps ① - ③, the practical Texas power grid is used to visualize the information needed for designing the MRGIoT attack strategy

network. By tracing the transmission routes from power plants to distribution substations, an attacker can accurately reconstruct the complete system graph.

Real-time power supply and demand data acquisition stage

Attackers can monitor grid operating conditions by leveraging publicly available data streams in deregulated electricity markets. Real-time information is typically refreshed every five minutes on Independent System Operator (ISO) platforms (see Supplemental Note 7). Global services including ELECTRICITY MAPS,[64] although updated less frequently, provide valuable high-level insights into regional power flows that support broader strategic assessments. Beyond these direct measurements, short-term forecasting approaches[70] that integrate live data, historical data patterns, and weather conditions often outperform native ISO forecasts for predicting system demand and intermittently available renewable generation. Furthermore, continuous access to real-time power flow data enables adversaries to infer underlying network topology by revealing spatial and temporal patterns of power distribution across transmission corridors.[71]

High-value RGU target identification stage

We define each node as a site consisting of a high-voltage bus and its connected lower-voltage substations, and we rank these sites using two core metrics: node degree and regional load density, while excluding units whose active power falls below a significance threshold. Node degree serves as a primary indicator of structural importance, reflecting the extent of network connectivity, whereas regional load density, derived from local demand and geographic area, provides a more robust measure of demand concentration than regional generation-to-load ratios (see Supplemental Notes 2 for details). By jointly tracking seasonal variations in load density with static topological attributes, we identify periods of maximal system stress and high-degree, high-generation RGUs as targets for coordinated botnet deployment, thereby enhancing the precision and timing of the attack strategy. Our analy-

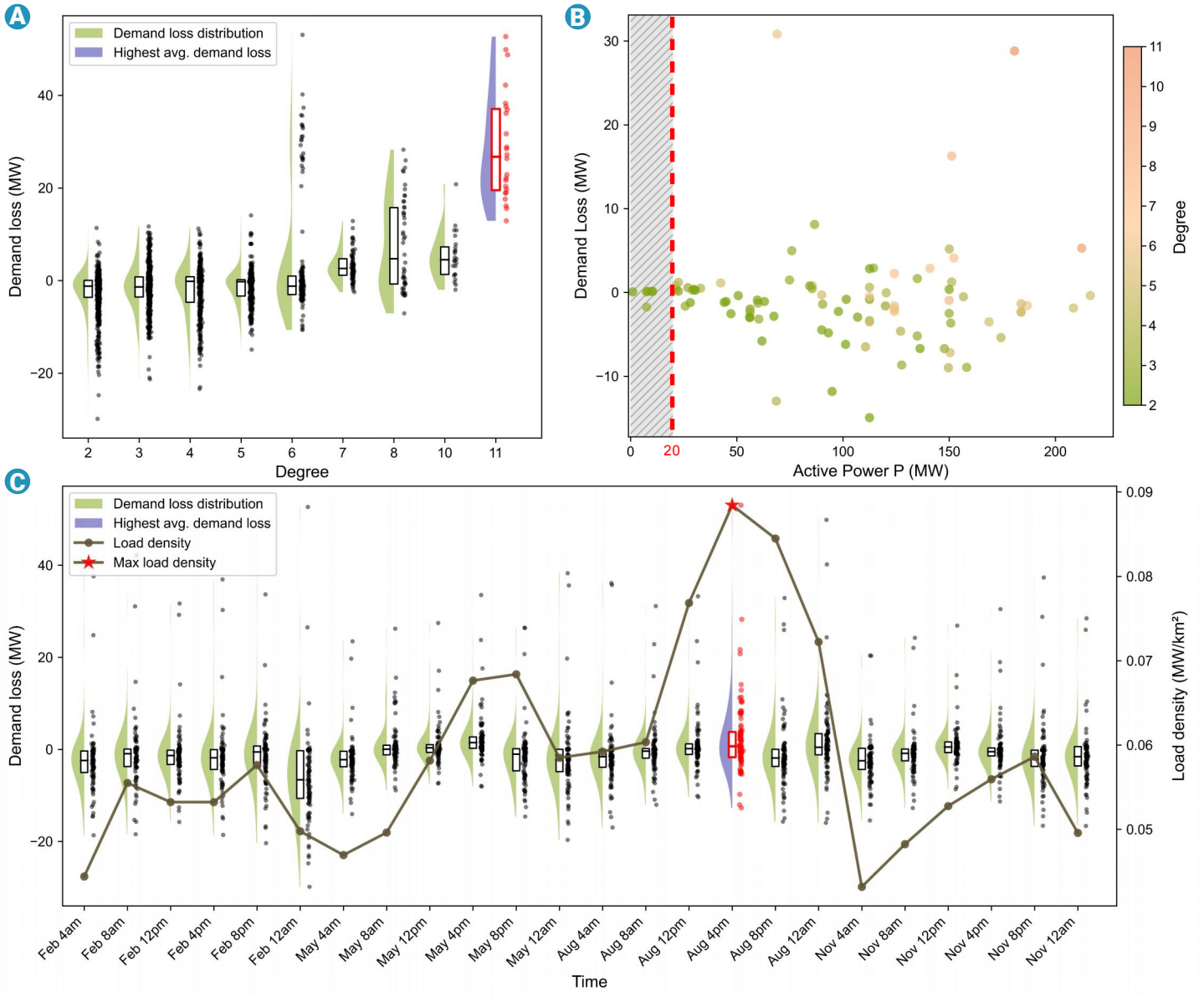

Figure 3. Sensitivity of attack impact (i.e., demand loss) to node degree, RGU output power, and attack time (A) Demand loss across the power grid caused by the attacks on RGUs with varying node degrees in the topology. The node degree associated with the highest average demand loss is highlighted in a distinct color. (B) Demand loss across the power grid caused by the attacks on RGUs with varying active power outputs. The region where the active power (P) is less than 20MW is highlighted with a gray shadow, and each point is colored according to its hosting node's degree. (C) Demand loss across the power grid caused by the attacks on different RGUs at 24 discrete time points throughout a year. The time associated with the highest average demand loss is highlighted in a distinct color. The line plot represents the grid's load density over the 24 time points, with the peak load density marked by a red pentagram. In summary, the results verify that the RGU targets with higher node degree, active output power, and load density normally lead to severe demand loss.

sis focuses on sites equipped with PV and WT installations, ensuring that both static topology and dynamic operating conditions inform target selection (see Supplemental Notes 1 for details).

Attack launch via pre-infected IoT botnets and pre-positioned physical attack devices

Attackers leverage detailed reconnaissance and analysis to orchestrate coordinated strikes on selected RGUs, deploying pre-infected IoT botnets such as Mirai[56] alongside pre-positioned physical devices. An IoT botnet attack typically involves three stages: compromising vulnerable devices, botnet formation and propagation, and command and control. They begin by exploiting weak credentials and unpatched software to compromise smart inverters, remote terminal units, cloud hosts, and smart loggers. These compromised assets form a rapidly expanding botnet that scans for additional vulnerabilities, after which a command-and-control (C&C) infrastructure directs distributed denial-of-service (DDoS) attacks, operational disruptions, data exfiltration, and precise manipulation of RGU power injections. As shown in Figure 2, multiple exploitable attack surfaces facilitate this process: smart inverters communicate with utility control systems via standards such as IEEE P2030.5/D4,[72] IEEE 1815[73] and SunSpec Modbus,[74] opening pathways for remote takeover;[75,76] widespread smart meter deployments expose state estimation to tampering;[77,78] and firmware modification or insecure monitoring interfaces provide further vectors. Although industrial control systems employ safeguards such as IEC 62443-compliant[79] air-gapped networks, zero-trust cloud platforms, and hardware security modules (HSMs), sophisticated adversaries can still mount advanced persistent threats,[80,81] exploiting supply-chain weaknesses, legacy protocol flaws, or insider credentials.

In parallel, adversaries can execute pre-deployed physical attacks against high-degree RGUs identified through topology data (Figure 2). Electromagnetic interference can inject bias signals into inverter sensors, corrupting controller inputs and triggering protection devices such as circuit breakers,[82–85] while forcible entry into turbine base cabinets allows compromise of fiber switches to disable entire wind farms.[86] This integrated cyber-

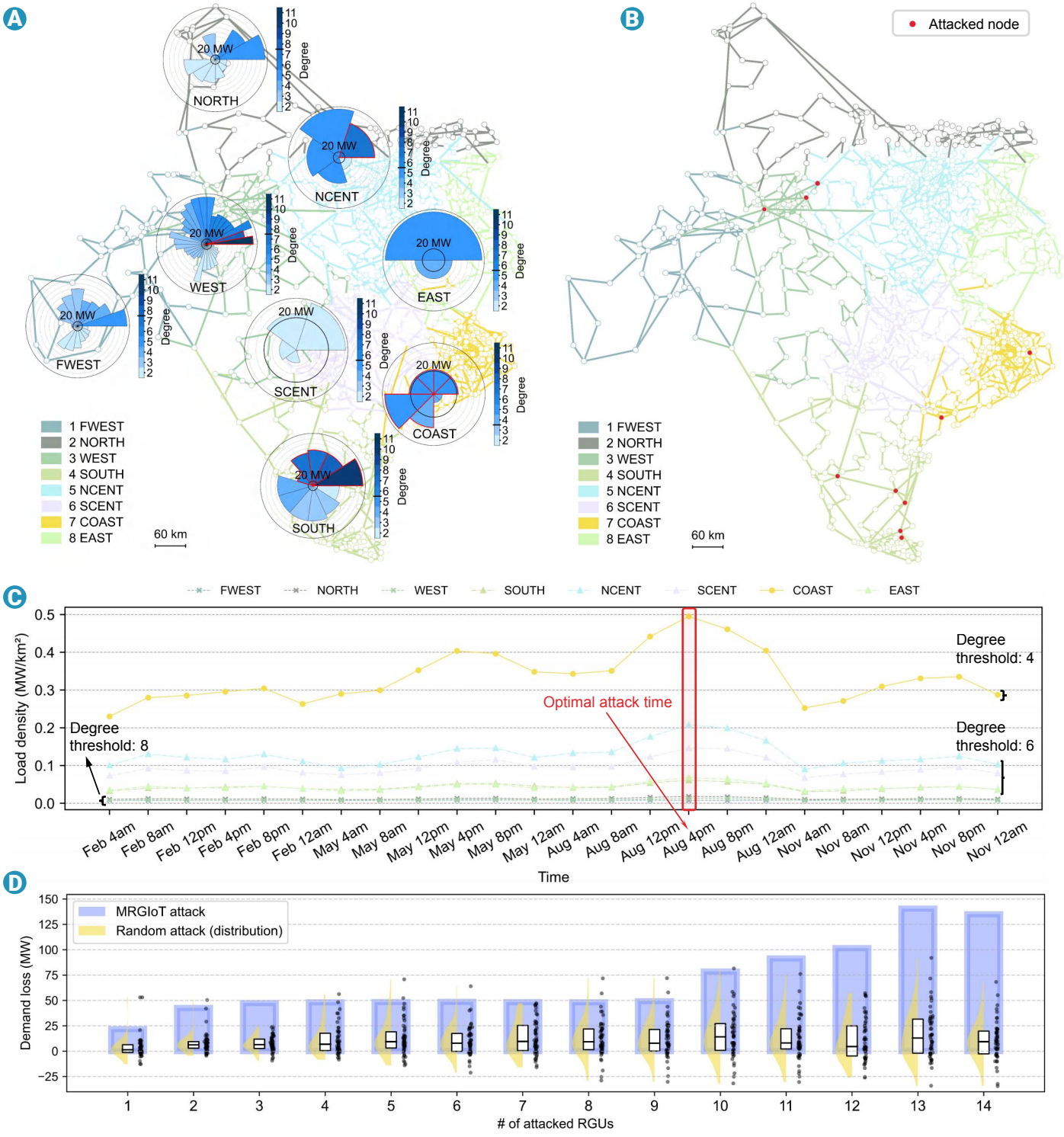

Figure 4. MRGIoT attack strategy design and corresponding impact analysis in the Texas power grid model (A) Demonstration of the selected RGU targets (with red outlines) based on the node degree, load density, and active output power. Each area uses a circle to illustrate the RGUs within it, with the color signifying the node degree and the radius representing the active output power, where the minimal 20 MW requirement is pictured using a smaller circle. (B) The spatial distribution of nodes hosting the selected RGU targets. (C) Fluctuations of load density across eight weather regions in the Texas power grid at 24 sampled time points throughout a year. Regions with higher load densities are assigned lower degree thresholds for RGU target selection. The time point with the highest load density is identified as the optimal attack time. d, Comparison of demand loss between MRGIoT attacks and 50 random attacks with the number of attacked RGUs ranging from one to fourteen.

physical strategy maximizes disruption by combining networked botnet attacks with targeted on-site interventions. Having outlined the MRGIoT framework, we next present experimental validation of its core system analysis stage and demonstrate the efficacy of proposed target selection metrics.

Impact of node degree and load density on target selection

Owing to the substantial economic and social impacts of real-world attacks, we employed the DIgSILENT PowerFactory[37] simulator to evaluate attack performance. The Texas grid model includes ninety-seven PV and WT generation units, providing an appropriately scaled and comprehensive platform for experimental analysis. To reflect actual grid conditions, we calibrated the model's generator and load profiles using hourly electricity supply

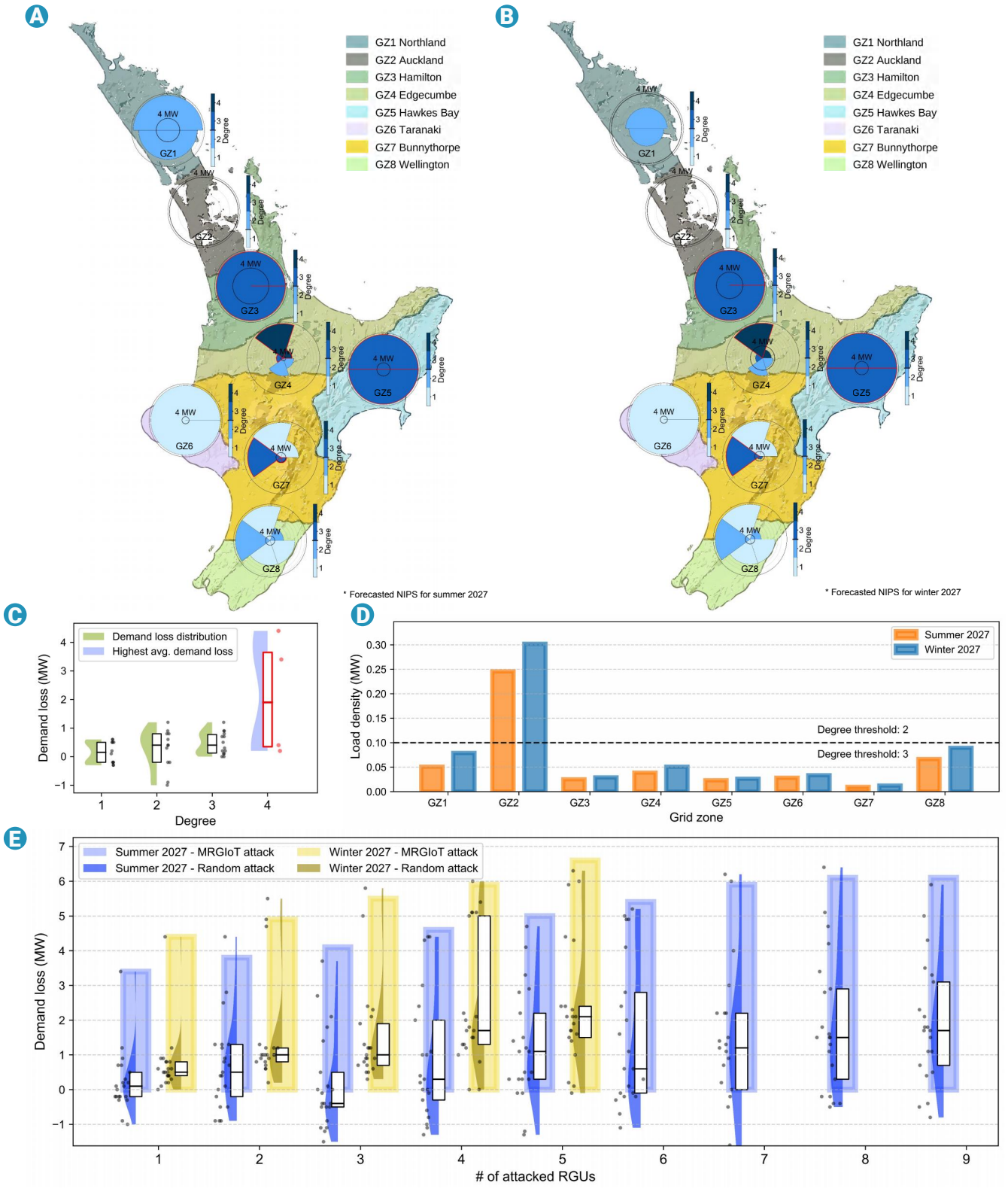

Figure 5. Impact of attack timing on MRGIoT effectiveness with a comparative analysis of summer and winter 2027 in the New Zealand North Island power system (A) and (B), Selected RGU targets of MRGIoT (with red outlines) under forecasted NIPS for summer 2027 (A) and winter 2027 (B). Each zone uses a circle to illustrate the RGUs within it, with the color signifying the node degree and the radius representing the active power output, where the black circle denotes the 4 MW minimum requirement. (C) Demand loss caused by attacks on RGUs with different node degrees. (D) Load density across eight grid zones under forecasted NIPS for summer and winter of 2027. Zones with higher load density are assigned lower degree thresholds. (E) Demand loss comparison between MRGIoT attack and 21 random attacks for summer and winter 2027, with the number of attacked RGUs ranging from one to nine

and demand data for Texas throughout 2023[88] (see materials and methods for details). We select four months and within each of these months we extract six time points, computing the mean supply and demand data across all days at each time to create twenty-four sampling scenarios for experi-

mental evaluation. At each sampling time point we manipulate every RGU in turn and recorded the resulting demand loss across the entire grid.

Statistical analysis shows that the attack-induced demand loss increases clearly with the node degree of RGUs and becomes dramatically higher at the very highest degrees (Figure 3A). Time-series analysis of attack outcomes reveals that disruption is greatest when grid load density reaches its peak (Figure 3C). However, the active power of RGUs ultimately governs attack impact: in the Texas grid model, the units with less than 20MW power generation cause negligible demand loss even when located at high-degree nodes (Figure 3B).

Analysis of MRGIoT attacks on the Texas grid model

The Texas grid model is partitioned into eight weather regions designated by ERCOT, each representing a geographical cluster with broadly similar climatic characteristics. Consequently, load density exhibits pronounced spatial and temporal variability across regions (Figure 4C). Analysis of twenty-four sampled time points across a full year identifies 4:00 pm in August as the moment of peak stress. Based on these load patterns, we derive region-specific node-degree thresholds for effective disruption: the COAST region, which exhibits the highest density, requires a minimum node degree of four; the NCENT, SCENT, EAST, and SOUTH regions require a degree of six or greater; and the NORTH, FWEST, and WEST regions require a threshold of at least eight. In addition to these topological constraints, targeted RGUs must exceed 20 MW of active power at the time of attack (Figure 4A). Applying these criteria, fourteen RGUs are ultimately selected from a pool of ninety-seven units, distributed across ten network nodes (Figure 4B).

To evaluate the effectiveness of the MRGIoT, we compare its resulting demand loss with that produced by random attacks under identical attack-budget constraints. The MRGIoT manipulates between one and fourteen RGUs. It prioritizes targets by first selecting units at the highest-degree nodes (e.g., nodes with degrees of ten or eleven). As the attack budget increases, additional RGUs are chosen by ranking regions in descending order of load density at the attack time and, within each region, selecting units according to node degree. The random benchmark follows the simple random sampling with fixed cost (SRSFC) method,[89] in which each RGU is selected with equal probability for a given budget. For each budget level, fifty independent random-attack trials are performed, and the corresponding demand loss is recorded to characterize the distribution of random outcomes. As shown in Figure 4D, the MRGIoT rapidly approaches the upper envelope of the fifty random-attack results as more RGUs are manipulated. Once the attack budget exceeds ten units, MRGIoT consistently and substantially outperforms random selection. These results demonstrate that the combined node-degree and load-density metrics offer a robust and discriminative basis for identifying the most influential RGUs, particularly when the defender's vulner-

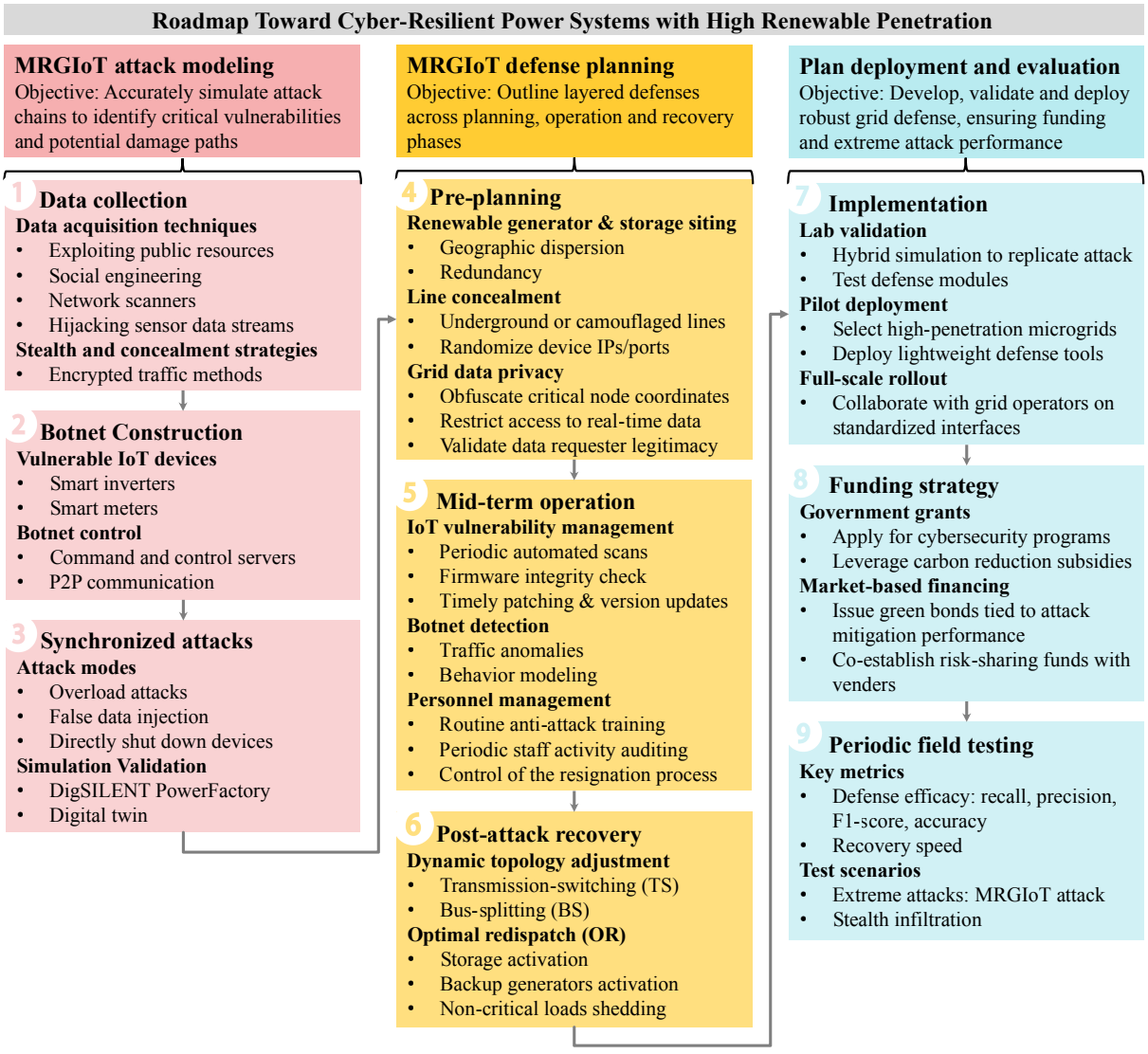

Figure 6. Roadmap toward cyber-resilient power systems The first step is to identify MRGIoT attack pathways that pose critical threats to power grids integrated with renewable energy resources. Following this, develop defense strategies for the construction, operational, and recovery phases - each tailored to the unique characteristics and progression of MRGIoT attacks. Finally, implement the comprehensive resilience plan and establish a full-life-cycle evaluation and optimization to ensure its long-term effectiveness and adaptability against evolving cyber threats.[91]

ability assessment encompasses more than ten units.

Analysis of MRGIoT attacks on the New Zealand North Island system

To further validate the effectiveness of the proposed MRGIoT framework and the impact of attack timing, another case study was conducted on the North Island power system (NIPS) of New Zealand, located in the Southern Hemisphere. Renewable energy development in New Zealand's North Island outpaces that of the South Island, with peak load density occurring in winter (Figure 5D). Consequently, according to the MRGIoT framework, the optimal attack timing is winter. Using the NIPS 2024 simulation model and 2027 forecast data, MRGIoT-based targeted attack analyses are performed for both summer and winter seasons. Solar power generation in winter is lower than in summer, and wind power output may also be partially reduced. As shown in Figures 5 A & B, the proposed selection strategy identifies nine high-impact RGUs in summer, but only five in winter. Although the number of high-impact nodes is smaller in winter, the higher load density during this season leads to greater attack impact. As illustrated in Figure 5E, demand loss caused by attacks launched in winter is consistently higher than that caused by attacks in summer. These results validate the rationality of the proposed MRGIoT framework, i.e., launching attacks at the time of peak load density. Furthermore, the statistical results from this case study again demonstrate the correlation between demand loss caused by attacks and the node degree of the attacked RGUs (Figure 5E). The grid zones used in this study are consistent with those defined on the Transpower official website.[90] For more experimental data, please download from the Data Availability.

Countermeasure recommendations

Our analysis shows that RGUs located in regions of high load density and at network nodes with high-degree exert disproportionately large system impacts when compromised, particularly during peak-demand periods. These findings motivate a layered defense strategy aimed at strengthening cyber resilience and operational robustness. First, RGUs at high-degree nodes within high-density regions should be prioritized for enhanced protection, as their compromise would pose the greatest systemic risk. Second, the visibility of critical infrastructure should be reduced through strategic concealment and information-minimization practices, thereby limiting adversarial reconnaissance and hindering the accurate mapping of key grid assets. Third, stringent security maintenance, including routine field inspections, continuous monitoring, and disciplined patch management for IoT-connected inverters, controllers, and sensors, is essential to detect unauthorized devices, remediate vulnerabilities, and prevent botnet infiltration. Fourth, access to real-time power-flow and demand data should be restricted to deprive attackers of the situational awareness required to precisely timed coordinated manipulations. Fifth, deploying flexible backup resources, such as fast-responding generation or energy storage,[92] can help maintain frequency stability when even a small number of RGUs are compromised in high-penetration renewable environments. Finally, integrated incident-response frameworks[93] that tightly couple cyber forensics, physical recovery actions, and system-level restoration procedures are needed to ensure rapid containment and resilient recovery under extreme attack scenarios.

These recommendations align with long-term objectives for net-zero development and high-penetration renewable deployment.[94] They help preserve continuous and secure grid operation even under adversarial conditions or unforeseen disruptions. In parallel, traditional siting principles and optimal grid-planning methodologies[95–97] must be reconsidered in light of emerging cyber-physical risks. To guide this transition, we propose a comprehensive resilience roadmap (Figure 6) that spans system construction, operation, and recovery, ensuring adaptive protection against evolving large-scale IoT-enabled threats.

DISCUSSION

The MRGIoT framework demonstrates a potent cyber-physical threat to RGU-dominated power systems by leveraging IoT botnets to compromise large numbers of renewable resources. The attack progresses through sequential stages of topology mapping, power data collection, system analysis and coordinated execution, enabling adversaries to exploit macro-level insights into grid structure and dynamics. By prioritizing targets according to node degree and regional load density, attackers can destabilize power system with far fewer compromised units than random strategies would require. At a renewable penetration of 42.8%, disabling only 12.3% of total generation capacity suffices to trigger a grid-wide collapse. These results highlight the critical need to embed targeted vulnerability assessments within security planning for renewable-dominated networks. The risk may escalate further if similar techniques were applied to high-voltage direct current (HVDC) links[98] that underpin long-distance transmission, potentially driving reliance on expensive backup resources and distorting market dynamics to the detriment of overall reliability.

Looking forward, research must focus on fortifying IoT-connected generation units through resilient communication protocols that ensure confidentiality, integrity, and availability (CIA), as well as real-time anomaly detection and predictive control schemes that enable timely and appropriate protective responses. The effectiveness of detection and control strategies ultimately depends on the availability and integrity of measurement data, which are constrained by system observability and monitoring infrastructure. Such measurements include not only electrical phasor data from phasor measurement units (PMUs) but also meteorological data from dedicated weather sensors. PMUs, as a key component of this monitoring infrastructure, are essential for detecting abnormal grid conditions but remain vulnerable to cyber-attacks, and their observability benefit hinges on appropriate placement.[99,100] Weather sensors, similarly, are critical for dynamic line rating (DLR) and renewable generation forecasting, yet their deployment and cyber protection have received less attention. Therefore, the vulnerable RGUs and surrounding areas identified in this study should be prioritized for enhanced sensor and PMU deployment and protection. Such targeted reinforcement of measurement infrastructure would directly improve the effectiveness of DLR and system integrity protection schemes (SIPS) by ensuring reliable data inputs for real-time anomaly detection, and coordinated control actions.[101,102]

In addition, the emerging use of intelligent algorithms and machine learning in grid operation introduces a dual-edged relationship with the MRGIoT threat framework. On the defensive side, system operators can proactively leverage machine learning to undermine the reconnaissance stages of MRGIoT. Adversarial perturbations can be deliberately injected into publicly accessible data streams such as grid topology information and real-time operational data published on ISO websites without compromising utility for legitimate users.[103] By applying such perturbation techniques before data release, operators could render the information collected by adversaries during MRGIoT Stages I and II systematically unreliable, thereby preventing attackers from deriving accurate vulnerability assessments during Stage III system analysis and fundamentally neutralizing the targeting advantage of MRGIoT. Furthermore, a machine learning-based classification framework that achieves perfect false negative rates and near-instantaneous detection of false data injection attacks could be deployed as a real-time protective layer during MRGIoT Stage IV, enabling rapid identification and mitigation of coordinated RGU manipulations before they cascade into system-wide disturbances.[104] On the adversarial side, the same machine learning technologies that enable these defenses also introduce new vulnerabilities. Deep reinforcement learning based controllers increasingly deployed in smart inverters and other grid-edge equipment are highly susceptible to adaptive gradient perturbation attacks.[103] An adversary who has already compromised RGUs via IoT botnets during MRGIoT Stage IV could augment their attack with DRL-generated adversarial inputs, deliberately corrupting the situational awareness of nearby intelligent controllers and amplifying the impact of RGU power manipulations beyond the directly compromised units. Thus, while machine learning offers powerful tools to fortify defenses across the MRGIoT attack chain, its growing presence in operational grid infrastructure simultaneously expands the attack surface available to sophisticated adversaries. This duality underscores that research on machine learning in relation to IoT-based manipulation of renewable generation units must continue to evolve on both fronts: developing adversarially resilient learning-based defenses while anticipating how emerging AI capabilities may empower next-generation variants of the MRGIoT framework.

CONCLUSION

In summary, MRGIoT provides a systematic framework comprising four

sequential stages including topology data acquisition, real time power supply and demand data acquisition, system analysis for high value target identification, and coordinated attack launch via IoT botnets. Using the Texas and New Zealand North Island power systems, MRGIoT demonstrates that RGUs located at high degree nodes and in high load density regions during peak periods will cause significant demand loss. Based on these findings, MRGIoT informs a set of targeted countermeasures including prioritizing high-degree RGUs within high density regions for enhanced protection, reducing the visibility of critical infrastructure through strategic concealment and information minimization practices, enforcing stringent security maintenance such as routine field inspections and disciplined patch management for IoT connected inverters, and restricting access to real time power flow and demand data to deprive adversaries of situational awareness. This study aims to fill the identified gap by providing the first framework that systematically evaluates which RGUs and under what conditions will pose the greatest threat to grid stability, thereby offering a rigorous foundation for developing effective cyber defense strategies.

REFERENCES

1. Ritchie H., Roser M. and Rosado P. (2024). Renewable Energy. *Our World in Data*. https://ourworldindata.org/renewable-energy
2. Nijsse F. J. M. M., Mercure J.-F., Ameli N., et al. (2023). The momentum of the solar energy transition. *Nat. Commun.* **14**:6542. DOI:10.1038/s41467-023-41971-7
3. SEIA. (2025). Solar energy industries association. *SEIA*. URL https://seia.org/
4. Slakaityte V., Surwillo I. and Berling T. V. (2023). A new cooperation agenda for european energy security. *Nat. Energy* **8**:1051–1053. DOI:10.1038/s41560-023-01322-8
5. Harnden T. (2002). Al-Qa'eda plans cyber attacks on dams. *Telegraph*. https://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1398683/Al-Qaeda-plans-cyber-attacks-on-dams.html
6. Poulsen K. (2003). Slammer worm crashed Ohio nuke plant net. *The Register*. https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_nuke/
7. Poulsen K. (2009). Report: Cyber attacks caused power outages in Brazil. *Wired*. https://www.wired.com/2009/11/brazil/
8. Meserve J. (2007). Staged cyber attack reveals vulnerability in power grid. *CNN*. https://edition.cnn.com/2007/US/09/26/power.at.risk/index.html
9. Kushner D. (2013). The real story of Stuxnet. *IEEE Spectrum*. https://spectrum.ieee.org/the-real-story-of-stuxnet
10. BBC. (2011). Iran says it has controlled Duqu malware attack. *BBC*. https://www.bbc.com/news/technology-15721839
11. BBC. (2012). Shamoon virus targets energy sector infrastructure. *BBC*. https://www.bbc.com/news/technology-19293797
12. CISA. (2021). Chinese gas pipeline intrusion campaign. *CISA*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a
13. Goodin D. (2014). Attackers poison legitimate apps to infect industrial systems. *Ars Technica*. https://arstechnica.com/information-technology/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/
14. Khandelwal S. (2014). Dragonfly hackers target energy firms. *The Hacker News*. https://thehackernews.com/2014/07/dragonfly-russian-hackers-scada-havex.html
15. Khandelwal S. (2014). South Korean nuclear plant hacked. *The Hacker News*. https://thehackernews.com/2014/12/Korea-nuclear-power-plant-hacked.html
16. Wikipedia. (2025). 2015 Ukraine power grid hack. *Wikipedia*. https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack
17. Wikipedia. (2025). 2016 Kyiv cyberattack. *Wikipedia*. https://en.wikipedia.org/wiki/2016_Kyiv_cyberattack
18. Greenberg A. (2017). Hackers found they could attack wind farms. *Wired*. https://www.wired.com/story/wind-turbine-hack/
19. Nakashima E. (2017). US officials say Russian hackers penetrated energy networks. *Washington Post*. https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638a-11e7-8adc-fea80e32bf47_story.html
20. Boren Z. (2018). Dragonfly UK energy hack. *Unearthed*. https://unearthed.greenpeace.org/2018/06/11/dragonfly-uk-energy-hacker-cybersecurity/
21. Geman B. (2018). Russia cyber war targeted grid. *Axios*. https://www.axios.com/2018/03/16/us-says-russias-cyber-war-targeted-the-grid-1521201831
22. Addison R. (2018). UK power grid cyber attack. *Industrial Cyber*. https://industrialcyber.co/threats-attacks/u-k-power-grid-hit-by-cyber-attack/.
23. National Cyber Security Centre. (2018). UK exposes Russian cyber attacks. *UK Gov*. https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks
24. Jones T. (2018). Hackers obtain nuclear plant plans. *DW*. https://www.dw.com/en/hackers-obtain-nuclear-power-plants-in-france/a-46126878
25. Austin P. (2021). Norsk Hydro ransomware attack. *Time*. https://time.com/6080293/norsk-hydro-ransomware-attack/
26. Asokan A. (2019). US energy utilities targeted by malware. *GovInfoSecurity*. https://www.govinfosecurity.com/us-energy-utilities-targeted-by-flowcloud-malware-a-14405
27. Paganini P. (2019). sPower cyber attack. *Security Affairs*. https://securityaffairs.com/93271/hacking/spower-cyber-attack.html
28. Monkey Cage. (2019). Indian nuclear plant cyberattack. *Washington Post*. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/
29. Owens C. (2019). Johannesburg electricity cyberattack. *Blackout Report*. https://www.theblackoutreport.co.uk/2019/07/29/johannesburg-ransomware-attack-july-2019/
30. Blaze Labs. (2020). Ragnar Locker case study. *Blaze Infosec*. https://www.blazeinfosec.com/post/dissecting-ragnar-locker-edp/
31. Paganini P. (2020). Sodinokibi ransomware attack. *Security Affairs*. https://securityaffairs.com/105477/cyber-crime/sodinokibi-ransomware-light-s-a.html
32. Nakashima E. and Timberg C. (2020). Russian hackers breach US agencies. *Washington Post*. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
33. Greenberg A. (2021). Russia GRU hackers targeted US grid. *Wired*. https://www.wired.com/story/russia-gru-hackers-us-grid/
34. Riis A. (2021). Cyber incident report. *Vestas*. https://www.vestas.com/en/media/company-news/2021/third-update-on-cyber-incident-c3466518
35. CS Energy. (2021). Cyber security incident response. *CS Energy*. https://www.csenergy.com.au/news/cs-energy-responds-to-cyber-security-incident
36. Fuentes M. (2021). Fire and cyberattack cause blackout. *Wise Plant*. https://wiseplant.com/a-fire-and-cyberattack-cause-major-blackouts-across-puerto-rico-2/
37. Morhan S. (2024). Meter tampering surge. *The Sun*. https://thesun.my/malaysia-news/tnb-s-collaboration-with-authorities-has-led-to-a-surge-in-detected-meter-tampering-cases-PE12437945
38. Wikipedia. (2022). Viasat hack. *Wikipedia*. https://en.wikipedia.org/wiki/Viasat_hack
39. Paganini P. (2022). Nordex cyber attack. *Security Affairs*. https://securityaffairs.com/129875/security/a-cyber-attack-forced-the-wind-turbine-manufacturer-nordex-group-to-shut-down-some-of-it-systems.html
40. Engdahl T. (2022). Ukraine power grid cyber attack. *Epanorama*. https://www.epanorama.net/blog/2022/04/13/cyber-attack-against-electrical-power-grid-in-ukraine/
41. Rojoef M. (2023). Russian hackers behind Ukrainian power outage. *Defense Post*. https://thedefensepost.com/2023/11/10/ukraine-2022-power-outage-russia/
42. Townsend K. (2022). Chinese hackers target energy firms in South China Sea. *SecurityWeek*. https://www.securityweek.com/chinese-hackers-target-energy-firms-south-china-sea/
43. CBC. (2023). Cyberattack hits Nunavut energy company. *CBC News*. https://www.cbc.ca/news/canada/north/qulliq-energy-corporation-cyberattack-1.6720056
44. Joncas H., Ferah M. and Marquis M. (2023). Hydro-Québec website cyberattack. *La Presse*. https://www.lapresse.ca/actualites/2023-04-13/cyberattaque/le-site-web-d-hydro-quebec-paralyse.php
45. Greenberg A. (2023). China-linked hackers breached power grid again. *Wired*. https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/
46. Antoniuk D. (2024). Russian citizen faces trial for power grid hack. *The Record*. https://therecord.media/russian-alleged-hack-power-grid
47. Toulas B. (2023). Slovenia power provider hit by ransomware. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/
48. Antoniuk D. (2023). Danish energy firms hacked via firewall bug. *The Record*. https://therecord.media/danish-energy-companies-hacked-firewall-bug
49. The Judean Staff. (2023). Red Evil cyber attack on Iran. *The Judean*. https://thejudean.com/index.php/news/science-technology/1971-pro-israel-hacker-group-red-evil-strikes-iran-with-second-cyber-attack
50. nquiringminds. (2024). Iranian cyber group develops IOControl malware. *Cyber News*. https://nquiringminds.com/cybernews/headline-iranian-cyber-group-develops-iocontrol-malware-targeting-critical-infrastructure/
51. CONTEC. (2024). Cyber attack on solar monitoring systems. *CONTEC*. https://www.contec.com/jp/info/2024/2024050700/
52. Maundrill B. (2024). Russian hackers target Ukrainian servicemen. *Cyber Report*. https://shturl.cc/C5c3Y0xVpUqNBAe4ezDF5tfCnqezGbj6a1IUDyWmoKPcHsb67l9JkPb2a8zSpSZHUf.
53. Schneider Electric. (2024). Cybersecurity incident report. *Schneider Electric Newsroom*. https://www.se.com/ww/en/about-us/newsroom/news/press-releases/sustainability-business-division-of-schneider-electric-responds-to-cybersecurity-incident-65b8035eb11dced626091019
54. Public Power. (2024). Cybersecurity wake-up call for utilities. *Public Power*. https://www.publicpower.org/periodical/article/cybersecurity-wake-call-lessons-attack-small-utility.
55. Jimada-Ojuolape B. and Teh J. (2020). Reliability impacts of cyber-physical power systems. *Sustain. Cities Soc.* **62**:102384. DOI:10.1016/j.scs.2020.102384

56. Antonakakis M., April T., Bailey M., et al. (2017). Understanding the Mirai botnet. *USENIX Security Symposium* **26**:1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis
57. Mohsenian-Rad A. H. and Leon-Garcia A. (2011). Load altering attacks in smart grids. *IEEE Trans. Smart Grid* **2**:667–674. DOI:10.1109/TSG.2011.2160297
58. Soltan S., Mittal P. and Poor H. V. (2018). BlackIoT botnet attacks on power grid. *USENIX Security Symposium* **27**:15–32. https://www.usenix.org/conference/usenixsecurity18/presentation/soltan
59. Shekari T., Cardenas A. A. and Beyah R. (2022). MaDIoT 2.0: IoT botnet attacks. *USENIX Security Symposium* **31**:3539–3556. https://www.usenix.org/conference/usenixsecurity22/presentation/shekari
60. Shekari T., Irvene C., Cardenas A. A., et al. (2021). MaMIoT energy market manipulation. *ACM CCS* **2021**:1338–1356. DOI:10.1145/3460120.3484581
61. Alexander O., Belisle M. and Steele J. (2020). MITRE ATT&CK for ICS. *MITRE Report*. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf
62. Google. (2025). Google Maps. *Google*. https://www.google.com/maps/
63. Rosvall R., Scholtes I. and Lambiotte R. (2019). Higher-order network models. *Nat. Phys.* **15**:313–320. DOI:10.1038/s41567-019-0459-y
64. Electricity Maps. (2025). Electricity grid visualization. *Electricity Maps*. https://app.electricitymaps.com/map
65. Wang Z., Scaglione A. and Thomas R. J. (2010). Power grid centrality measures. *IEEE CDC* **2010**:5792–5797. DOI:10.1109/CDC.2010.5717964
66. Rosas-Casals M., Valverde S. and Solé R. V. (2007). European power grid vulnerability. *Int. J. Bifurc. Chaos* **17**:2465–2475. DOI:10.1142/S0218127407018531
67. Wang Z., Scaglione A. and Thomas R. J. (2010). Grid robustness analysis. *IEEE ICC Workshops* **2010**:1–5. DOI:10.1109/ICCW.2010.5503926
68. Keliris A., Konstantinou C., Sazos M., et al. (2019). OSINT for energy cyberattacks. In *Critical Infrastructure Security and Resilience* (Springer), pp:261–281. DOI:10.1007/978-3-030-00024-0_14
69. Singh A. K., Ibraheem, Khatoon S., et al. (2012). Load forecasting techniques review. *IEEE ICPCES* **2012**:1–10. DOI:10.1109/ICPCES.2012.6508132
70. Li X., Poor H. V. and Scaglione A. (2013). Power system topology identification. *SmartGridComm* **2013**:91–96. DOI:10.1109/SmartGridComm.2013.6687939
71. IEEE. (2023). IEEE P2030.5 smart energy profile. *IEEE Std*. https://ieeexplore.ieee.org/servlet/opac?punumber=10289673
72. IEEE. (2012). DNP3 communication standard. *IEEE Std 1815-2012*. DOI:10.1109/IEEESTD.2012.6327578
73. Colak A. M., Tawada Y., Inzunza R., et al. (2021). Modbus-TCP photovoltaic inverters. *ICRERA* **2021**:111–115. DOI:10.1109/ICRERA52334.2021.9598491
74. Ahn B. H., Kim T., Ahmad S., et al. (2024). Cyber-resilient smart inverters. *IEEE Trans. Power Electron.* **39**:4657–4673. DOI:10.1109/TPEL.2023.3342842
75. Daniel dos Santos F. L. S. (2025). Solar system vulnerabilities. *BlackHat Asia*. https://www.blackhat.com/asia-25/briefings/schedule/#a-closer-look-at-the-gaps-in-the-grid-new-vulnerabilities-and-exploits-affecting-solar-power-systems-43223
76. Liu Y., Ning P. and Reiter M. K. (2011). False data injection attacks. *ACM Trans. Inf. Syst. Secur.* **14**:1–33. DOI:10.1145/1952982.1952995
77. Sun C.-C., Cardenas D. J. S., Hahn A., et al. (2021). Smart meter intrusion detection. *IEEE Trans. Smart Grid* **12**:612–622. DOI:10.1109/TSG.2020.3010230
78. ISA Global Cybersecurity Alliance. (2025). ISA/IEC 62443 standards. *ISA GCA*. URL https://isagca.org/isa-iec-62443-standards
79. Chen P., Desmet L. and Huygens C. (2014). Advanced persistent threats study. In *CMS 2014* (Springer), pp:63–72.
80. Alshamrani A., Myneni S., Chowdhary A., et al. (2019). Survey on APTs. *IEEE Commun. Surveys Tuts.* **21**:1851–1877. DOI:10.1109/COMST.2019.2891891
81. Alshamrani A., Myneni S., Chowdhary A. and Huang D. (2019). A survey on advanced persistent threats. *IEEE Commun. Surv. Tutor.* **21**:1851–1877. DOI:10.1109/COMST.2019.2891891
82. Barua A. A. and Faruque M. A. A. (2020). Hall spoofing: A non-invasive DoS attack on grid-tied solar inverter. *USENIX Security Symposium* **29**:1273–1290. https://www.usenix.org/conference/usenixsecurity20/presentation/barua
83. Wang Z., Pan K. and Xu W. (2025). Sensor attacks on grid-tied photovoltaic inverters. *IEEE Trans. Ind. Inform.* **21**:820–829. DOI:10.1109/TII.2024.3463704
84. Dan Z., Yang F., Pan K., et al. (2022). EMI attack on photovoltaic inverter control systems. *IEEE EI2* **2022**:1076–1080. DOI:10.1109/EI256261.2022.10116254
85. Yang F., Dan Z., Pan K., et al. (2025). Electromagnetic interference attacks on power inverters. *NDSS Symposium* **2025**:24–28. DOI:10.14722/ndss.2025.23069
86. Staggs J., Ferlemann D. and Shenoi S. (2017). Wind farm security and attack surfaces. *Int. J. Crit. Infrastruct. Prot.* **17**:3–14. DOI:10.1016/j.ijcip.2017.03.001
87. DIgSILENT PowerFactory Dev. Core Team. (2022). DIgSILENT PowerFactory. *DIgSILENT*. URL https://www.digsilent.de/en/
88. ERCOT. (2025). Electric reliability council of Texas. *ERCOT*. URL https://www.ercot.com/
89. Singh S. and Singh S. (2003). Simple random sampling. *Adv. Samp. Theory* :71–136. DOI:10.1007/978-94-007-0789-4_2
90. Transpower New Zealand. (2026). Empowering our energy future. *Transpower*. https://www.transpower.co.nz/
91. Liu M., Teng F., Zhang Z., et al. (2024). Enhancing cyber-resiliency of DER-based smart grid. *IEEE Trans. Smart Grid* **15**:4998–5030. DOI:10.1109/TSG.2024.3373008
92. Wang R., Ji H., Li P., et al. (2024). Multi-resource coordinated planning of distribution networks. *Nat. Commun.* **15**:4576. DOI:10.1038/s41467-024-48862-5
93. Spyrou E., Hobbs B. F., Bazilian M. D. and Chattopadhyay D. (2019). Power system planning in fragile states. *Nat. Energy* **4**:300–310. DOI:10.1038/s41560-019-0346-x
94. Zappa W., Junginger M. and van den Broek M. (2019). 100% renewable European power system feasibility. *Appl. Energy* **233–234**:1027–1050. DOI:10.1016/j.apenergy.2018.08.109
95. Cao M., Guo J., Xiao H. and Wu L. (2022). Reliability analysis of non-repairable power systems. *Reliab. Eng. Syst. Saf.* **222**:108443. DOI:10.1016/j.ress.2022.108443
96. Wang R., Ji H., Li P., et al. (2024). Multiresource dynamic coordinated planning of flexible distribution network. *Nat. Commun.* **15**:4576. DOI:10.1038/s41467-024-48862-5
97. Xiao H. and Cao M. (2020). Reliability modeling and maintenance optimization. *Energy* **210**:118470. DOI:10.1016/j.energy.2020.118470
98. Hou J., Deng H. and Peng J. C.-H. (2024). Attack-induced equilibrium in HVDC systems. *IEEE Trans. Smart Grid* **15**:5992–6004. DOI:10.1109/TSG.2024.3409704
99. Jimada-Ojuolape B., Teh J. and Lai C.-M. (2025). PMU placement in cyber-physical grids. *Electric Power Syst. Res.* **241**:111327. DOI:10.1016/j.epsr.2025.111327
100. Jimada-Ojuolape B., Teh J. and Lai C.-M. (2024). Cybersecurity challenges in PMU systems. *Electric Power Syst. Res.* **233**:110509. DOI:10.1016/j.epsr.2024.110509
101. Jimada-Ojuolape B. and Teh J. (2022). Composite reliability of synchrophasor systems. *IEEE Syst. J.* **16**:3927–3938. DOI:10.1109/JSYST.2021.3132657
102. Lawal O. A. and Teh J. (2023). Reliability modeling of dynamic line rating. *Sustain. Energy Grids Netw.* **35**:101140. DOI:10.1016/j.segan.2023.101140
103. Su Y., Dai Z., Teh J., et al. (2026). Attack and defense in DRL-based grid reconfiguration. *Expert Syst. Appl.* **309**:131209. DOI:10.1016/j.eswa.2026.131209
104. Lawal O. A., Teh J., Alharbi B. and Lai C.-M. (2024). FDI attack mitigation in DLR systems. *Sustain. Energy Grids Netw.* **38**:101347. DOI:10.1016/j.segan.2024.101347
105. Chen D., Lü L., Shang M.-S., et al. (2012). Influential node identification in complex networks. *Physica A* **391**:1777–1787. DOI:10.1016/j.physa.2011.09.017
106. Delfino B., Massucco S., Morini A., et al. (2001). Under-frequency load shedding schemes. *In IEEE Power Engineering Society Summer Meeting* **2001**:307–312. DOI:10.1109/PESS.2001.970031
107. ICSEG. (2025). IEEE 39-bus system dataset. *ICSEG*. URL https://icseg.iti.illinois.edu/ieee-39-bus-system/
108. Electricity Authority NZ. (2025). PowerFactory case files. *EA NZ*. URL https://www.emi.ea.govt.nz/Wholesale/Datasets/Transmission/PowerSystemAnalysis/PowerFactoryCaseFiles

FUNDING AND ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China under Grant 62293503, 62293500, 62293502, in part by the Natural Science Foundation of Zhejiang Province under Grant LR23F030001, in part by the Frontier Technologies R&D Program of Jiangsu under Grant BF2024065, in part by the State Key Laboratory of Industrial Control Technology under Grant ICT2024A13, ICT2025C04, in part by the Xiaomi Foundation, and in part by the Fundamental Research Funds for the Central Universities 226-2025-00165.

AUTHOR CONTRIBUTIONS

Y.L. and R.D. designed the research; Y.L. and M.L. performed the investigation and validation; Y.L. prepared the original draft and conducted data curation; P.C. and J.C. acquired resources and secured funding; M.L., W.M., and R.D. reviewed and edited the manuscript. All authors contributed to discussions on the framework and to the editing of the article.

DECLARATION OF INTERESTS

The authors declare no competing interests.

ETHICAL STATEMENT AND PATIENT CONSENT

During the editing of the draft, the authors used ChatGPT for language readability improvement. The authors have carefully checked the manuscript and are responsible for the content.

DATA AND MATERIALS AVAILABILITY

The dataset to reproduce our results is available on Zenodo at https://zenodo.org/records/19794068. The Python code used to create our results and figures is also available on Zenodo at https://zenodo.org/records/19794143.

SUPPLEMENTAL INFORMATION

It can be found online at https://doi.org/10.59717/j.xinn-energy.2026.100169