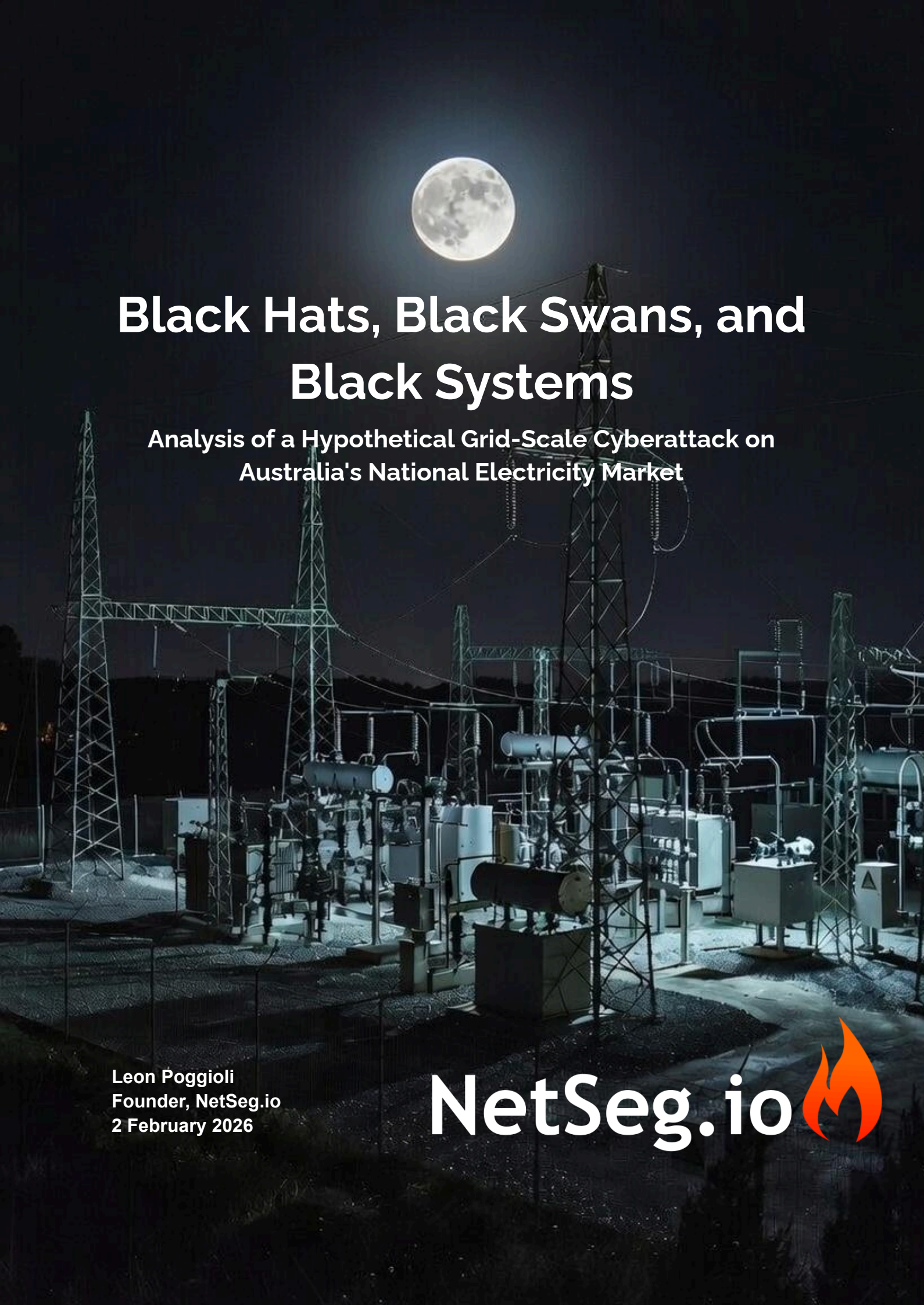

Black Hats, Black Swans, and Black Systems

Analysis of a Hypothetical Grid-Scale Cyberattack on Australia's National Electricity Market

Leon Poggioli
Founder, NetSeg.io
2 February 2026

NetSeg.io

Executive Summary

Australia's electricity grid is undergoing its most significant transformation since electricity became widely available. The rapid shift from centralised fossil fuel generation to distributed renewable energy sources (DER) has accelerated decarbonisation efforts, but has also introduced new cyber-risks and fragilities that nation-state actors and cyber-terrorists could exploit to devastating effect.

This paper models a realistic worst-case scenario: a coordinated cyberattack designed to trigger a grid-scale blackout across Australia's National Electricity Market (NEM). Our analysis draws on historical grid failures, current threat intelligence, and the physical realities of frequency control in power grids with a high penetration of DER.

Some readers may think such an event to be too unlikely to warrant a whitepaper, but as was observed in the 2025 Iberian power grid collapse[1], as the world moves away from inertia-based power sources to DER, the risk of a grid collapse increases. Most recently, a cyberattack specifically targeting DER was observed in Poland[23]. These events may be infrequent, but they are Black Swans - unpredictable and with extreme consequences.

This paper explores the NEM's fragility to a cyberattack and ways to make the NEM more robust to long tail events like black system events, using publicly available information.

Key findings:

- A targeted cyberattack during a peak demand period, aimed at taking generation capacity offline during such periods could cause a frequency deviation below 47-48 Hz could cause a black system across individual states or even the entire NEM.
- The motivation for such an attack would be more likely to be an act of cyber-terrorism or cyber-warfare to achieve geopolitical objectives rather than financial extortion by organised crime.
- The optimal attack window would be during a summer heatwave when demand on the NEM peaks above 40GW - either around 1PM during peak solar contribution, or 7PM when solar generation tapers off but demand remains high.
- The economic impact of a medium-scale attack targeting a single region is estimated at AUD $2-8 billion.
- Potential indirect fatalities from a sustained outage: 0-50 lives, primarily vulnerable populations, depending on services affected.
- The Security of Critical Infrastructure (SOCI) Act now mandates that energy market participants implement robust cyber risk management programs. However, many smaller operators, primarily running DER systems, lack the OT security maturity to invest in such controls and withstand sophisticated, coordinated attacks.

This paper provides a foundation for understanding the cyber risk factors of a DER-heavy grid and offers recommendations for increasing resilience against a target cyberattack across the NEM.

Introduction

Cybersecurity of critical infrastructure has captured the attention of governments worldwide. Critical infrastructure is generally defined as any piece of infrastructure the public relies on to live in a modern civilisation - such as airports, basic utilities like water, power, and phone, banking, supermarkets and the associated supply chains these infrastructures rely on.

In Australia, the Security of Critical Infrastructure (SOCI) Act 2018 - significantly strengthened in 2022 and 2024[4] - now imposes mandatory obligations on operators of critical infrastructure assets, including cyber incident reporting within 12-72 hours and implementation of Critical Infrastructure Risk Management Programs (CIRMPs). There are now proposed enhancements to the CIRMP tabled for consultation from the Department of Home Affairs.[5]

Certain assets have been designated as "Systems of National Significance" - those pieces of critical infrastructure that play the most vital roles in maintaining Australia's way of life. The electricity grid sits at the foundation of all critical infrastructure, as prolonged power outages cascade immediately into failures across telecommunications, water treatment, groceries healthcare, transport, and finance.

Reliable access to electricity underpins every element of modern civilisation.

Why Now?

The urgency stems not merely from high-profile incidents like the Ukrainian power grid attacks of 2015 and 2016, and the more recent attacks on Poland’s DER systems on December 29, 2025, but from fundamental changes in how our grid operates:

Less built-in inertia: Electrical grid inertia is like the momentum that keeps a spinning top stable - it's the built-in resistance of the power system to sudden changes in frequency caused by imbalances between electricity supply and demand, helping prevent blackouts or instability. Stable frequency control (at 50Hz in Australia) is critical for grid stability. In traditional base-load systems powered by coal-fired power stations, inertia comes naturally from the massive spinning turbines and generators that rotate synchronously with the grid's frequency. These heavy rotating masses store kinetic energy and automatically release or absorb it to smooth out fluctuations, acting as a buffer during faults or load changes.

Modern renewable-heavy grids, dominated by solar panels and wind turbines, often lack this inherent inertia because they connect via electronic inverters that don't have physical spinning parts, making the system more vulnerable to rapid frequency swings as renewables can vary quickly with weather. To compensate in these modern systems, engineers must add artificial inertia through technologies like synchronous condensers (spinning machines without power output), flywheels that store rotational energy, or Battery Energy Storage Systems (BESS) with grid-forming inverters that mimic traditional inertia by rapidly injecting or withdrawing power to stabilize the grid.

Dynamic Grid Operation: Modern power grids increasingly less dependent on base load generation with in turn a higher dependency on rely on VRE (Variable Renewable Energy) sources such as wind and solar, vs traditional base load energy sources like coal. As well as artificial inertia sources, these Distributed Energy Resources (DER) require more market interventions to maintain grid stability rather than traditional fossil-fuel based base load generation like coal. Renewable energy now accounts for 60-70+% of NEM generation during peak demand periods.

New Data Centres: The rise of AI has driven record new data centre builds, with ever-increasing demands for power. NEM-connected Data Centres currently account for 2% of power consumption on the NEM, this is expected to grow to 6% by 2030, from 4 TWh to 12 TWH per annum. [6]

Increased automation: Modern grid management relies on digital control systems for efficiency, but these systems expand the attack surface particularly as they control down to home solar inverter level. This opens the avenue for attackers to manipulate signals of instructions that feed systems like Virtual Power Plants (VPP) and cause frequency instability. [7]

Supply chain integration: Operational Technology (OT) networks increasingly connect to IT systems and external vendors, expanding the attack surface and potential entry points for attackers. This interconnectivity is expected to continue as the grid supply systems continue to become more dynamic.

Evidence of Nation State compromise: Recent papers[8][9] have demonstrated that Nation State sponsored hacking groups such as Volt Typhoon have been shown to be nesting inside many American critical infrastructure operators, and evidence suggests a similar level of activity within Australia critical infrastructure operators.

This suggests two objectives: to undertake recon of weak points within the overall system, and to prepare for potential warfare with Australia where a nation state could trigger a cyberattack as retaliation against Australia, delivering destructive consequences to achieve geopolitical objectives.

As was observed in the Polska CERT report[3] the attackers were seen to have been conducting recon within grid systems for months before the attack was launched, activity which appears to be underway in Australia and other countries based on public reports.

Threat Actors and Motivations

While ransomware and data theft dominate cybercrime headlines, these attacks are fundamentally financially motivated. Attackers follow well-trodden paths that maximise profit while minimising the negative publicity associated with attacks on critical services.

Nation-state actors and cyber-terrorists - the key threat actors motivated to target critical infrastructure - operate under a different calculus. Their objectives are geopolitical: destabilisation, coercion, demonstration of capability, or preparation for kinetic conflict. For

these adversaries, a coordinated attack on Australia's electricity grid offers asymmetric impact - massive disruption from relatively modest investment.

Intelligence agencies including ASIO have publicly warned of pre-positioned access in Australian critical infrastructure by state-sponsored actors. The question is not whether adversaries have the capability to attack our grid, but when and whether they choose to act.

Understanding Grid Frequency Control

To understand how a cyberattack could destabilise the grid, we must first understand the physics of frequency control.

The 50 Hz Imperative

Australia's alternating current (AC) grid operates at a nominal frequency of 50 Hz - meaning the electrical current alternates direction 50 times per second. This frequency must be maintained within tight tolerances of +/- 0.015Hz with allowances for greater frequency deviations during system stabilisation and for temporary periods, such as when a system is operating in island mode.

When electricity supply and demand are perfectly matched, frequency remains stable at 50 Hz. When demand exceeds supply, frequency drops. When supply exceeds demand, frequency rises.

When frequencies deviate too far from the 50Hz target range, protection relays are tripped, and can cause cascading failures leading to large-scale blackouts and a “black system” event.

As highlighted earlier in this whitepaper, grid inertia was provided naturally in traditional base load systems that had physical components that were spinning to generate electricity. Modern renewable energy is inverter-based, so requires other systems to deliver inertia like BESS facilities. This means that much more effort is required to maintain frequency control in modern DER-heavy systems and a DER-heavy grid is more fragile to deviations from system frequency.

Frequency Control Ancillary Services (FCAS)

AEMO (The Australian Energy Market Operator - manager of the NEM) manages frequency through the Frequency Control Ancillary Services (FCAS) market, procuring fast-responding reserves to correct imbalances:

- Regulation services: Continuous small adjustments to match supply and demand
- Contingency services: Rapid response (6 seconds to 5 minutes) to significant events like generator trips
- System strength services: Maintaining the physical characteristics needed for stable operation

These services traditionally came from large synchronous generators (coal, gas, hydro) that provide "inertia" - physical resistance to frequency changes due to the rotating mass of their turbines. A grid with high inertia is more resistant to sudden frequency changes, giving operators time to respond.

The Low-Inertia Challenge

As synchronous generators retire and are replaced by inverter-based renewables (solar, wind, batteries), the grid loses inertia. In a low-inertia system:

- Frequency changes faster in response to supply-demand imbalances
- Rate of Change of Frequency (RoCoF) can exceed 3-6 Hz/second
- Traditional protection systems may not respond quickly enough
- Cascading failures can develop within seconds

The 2016 South Australia blackout demonstrated this vulnerability. When multiple wind farms disconnected during a severe storm, frequency collapsed at approximately 6 Hz/second — so fast that Under-Frequency Load Shedding (UFLS) could not arrest the decline before the system separated from the rest of the NEM and collapsed.

Black Start Capability

When a grid experiences complete collapse (a "black system" event), restoration requires "black start" capability - generators that can start without external power and progressively re-energise the network. Re-starting the power isn't a case of metaphorically "turning it back on again" - most power sources need initial input power to re-start, and the power generated needs a stable source of demand to maintain grid balance and frequency control as more power supplies are re-started and more of energy consumers are brought back onto the grid.

Grid operators like AEMO contract System Restart Ancillary Services (SRAS) from providers capable of black starts. However, restoration is slow (potentially 24-72 hours for full recovery), complex, and requires careful coordination to avoid triggering secondary collapses. The time lag to initiate a black start means that the impact of a black system is much more severe than a local blackout that results from a protection relay tripping. This becomes particularly complex when associated with a grid wide black system rather than a state level black system.

Such a long period without power could exhaust generator facilities at critical operations such as hospitals, and could lead to loss of life events, for example during heatwave situations where vulnerable members of the population can be affected by heatstroke when they can't run air conditioning.

As the grid transitions to renewables, black start strategies are evolving — with trials now exploring batteries and other modern technologies. However, a coordinated cyberattack could target both the systems that cause collapse and those needed for recovery.

Historical Grid-Scale Blackouts

While grid-scale blackouts are rare, their impacts are severe. Examining historical events reveals patterns that inform both natural vulnerabilities and potential attack vectors. Below are several examples of grid-scale blackouts from the past 15 years:

Iberian Peninsula Blackout (April 2025)

Duration: ~10 hours (core areas)
Affected Population: ~55 million (Spain, Portugal)
Economic Impact: €300+ million (insured losses)
Fatalities: 8 (candle fires, generator fumes)

Cause: Cascading transmission failure affecting mainland Portugal and Spain, with ripple effects in France and Andorra. The event disrupted essential services including healthcare systems.

Key Lesson: Even in modern, well-resourced grids, cascading failures can develop rapidly and overwhelm protection systems.[1]

Texas Power Crisis (February 2021)

Duration: 4-6 days (rolling blackouts)
Affected Population: ~4.5 million households
Economic Impact: USD $80-195 billion
Fatalities: 210-246 (estimated)

Cause: Winter Storm Uri brought extreme cold that froze natural gas infrastructure and caused widespread generation failures. The isolated Texas grid (ERCOT) could not import power from neighbouring systems.

Key Lesson: Grid isolation amplifies vulnerability. Single points of failure in fuel supply chains can cascade into generation shortfalls.[10]

South Australia Statewide Blackout (September 2016)

Duration: Hours to days (by area)
Affected Population: 1.7 million
Economic Impact: AUD $360+ million
Fatalities: 0 (direct)

Cause: Severe storms damaged transmission infrastructure. Multiple wind farms disconnected due to voltage disturbances. The resulting frequency collapse (nadir of 47-48 Hz) separated South Australia from the NEM, causing a black system across South Australia.

Key Lesson: High renewable penetration reduces system inertia. Rapid frequency changes can overwhelm protection systems before they can respond. This event directly informed subsequent reforms to generator technical standards.[11]

Ukraine Power Grid Cyberattacks (December 2015, December 2016)

Duration: 1-6 hours
Affected Population: ~230,000 customers
Economic Impact: Not quantified (primarily demonstration)
Fatalities: 0 (direct)

Cause: State-sponsored attackers used malware (BlackEnergy, Industroyer) to remotely operate circuit breakers at distribution companies, causing synchronised outages. Attackers also targeted backup systems and call centres to hinder recovery.

Key Lesson: Cyberattacks on grid infrastructure are not theoretical — they have been successfully executed. The attacks demonstrated capability while deliberately limiting impact; a full-scale attack could have been far more severe.[12]

India Grid Collapse (July 2012)

Duration: ~15 hours
Affected Population: 620+ million
Economic Impact: Hundreds of millions to billions USD
Fatalities: 0 (direct, though indirect effects likely)

Cause: Overloaded transmission lines and failure to properly island northern and eastern grids during successive disturbances led to cascading failure across 22 states — the largest blackout in history by population affected.

Key Lesson: Interconnected grids can propagate failures across vast areas. Coordination failures between grid operators amplify impact.[13]

Anatomy of a Grid-Scale Cyberattack

A sophisticated adversary seeking to cause maximum disruption to Australia's grid would likely combine multiple attack vectors, timed to exploit natural vulnerabilities. Based on publicly available threat intelligence and technical analysis, we can construct a realistic attack profile of what such a scenario might look like, and determine methods to reduce both the risk and impact of such an event.

Attack Objectives

A nation-state or well-resourced threat actor would likely seek to:

- Trigger cascading frequency deviation leading to regional or national blackout
- Maximise duration by targeting recovery systems alongside primary infrastructure
- Amplify secondary impacts across dependent sectors (telecommunications, water, healthcare)
- Use recon (done by nesting in energy sector OT environments) to identify the most vulnerable target points to cause instability.

Initial Access Vectors

Pre-positioned Espionage Access

Intelligence assessments indicate a high probability that state-sponsored actors have established foothold access to Australian critical infrastructure networks. This access - gained through supply chain compromises, spear-phishing, or exploitation of internet-facing systems - can remain dormant for months or years before activation. This problem is not unique to Australia and serves as further re-inforcement of the importance of continuous monitoring of these systems, even if they are intended to be run in an isolated fashion.

Attackers could leverage this access to:

- Map OT network architecture and identify critical control points
- Identify timing windows for maximum impact
- Prepare malware payloads tailored to specific systems
- Establish command-and-control channels that survive initial detection

Distributed Energy Resource Exploitation

Solar inverters, battery systems, and EV chargers represent a particularly attractive target as they often have less security visibility and control, and more external connectivity.

Scale: Millions of devices with network connectivity
Diversity: Hundreds of manufacturers with varying security postures
Vulnerability: These devices when housed in small-scale or home environments are less likely to be patched than in larger enterprise environments
Concentration: Many devices share common firmware vulnerabilities and are managed centrally by aggregation systems like VPPs
Access: Consumer devices often lack enterprise security controls and/or are incompatible with such controls.

Supply Chain Compromise

Hardware and software used in grid infrastructure passes through complex global supply chains.

This could include embedded backdoors in:

- Industrial control system components
- Network equipment in substations
- Monitoring and SCADA systems
- Smart meters and grid sensors
- Home solar inverters

These compromises may be undetectable until activated, potentially years after installation. It is worth noting that a supply chain compromise isn't the only mechanism through which supply chain can be used as a mechanism to launch a cyberattack.

Due to the long lifecycles of Operating Technology, a new security vulnerability on an End-of-life device could be sufficient to launch a new cyberattack, particularly if able to be launched on a large scale, for example tens of thousands of home solar inverters with the same make and model. This re-inforces the importance of maintaining asset inventory (including assets not directly owned by the entity, for example home solar inverters managed by a VPP), both to maintain asset currency and be able to respond quickly if a critical vulnerability with a known exploit is released.

Attack Techniques

The following methods could be used by attackers to destabalise grid systems. When performed at a large enough scale, targeted at the right pressure points during the right demand period, partial or total grid collapse can be triggered.

False Data Injection

Manipulating sensor data fed to Automatic Generation Control (AGC) or frequency monitoring systems can cause generators to over- or under-produce, creating real frequency deviations that cascade through the system.

Coordinated Load/Generation Manipulation

Simultaneously commanding compromised DER devices to disconnect (or surge output) can create instantaneous supply-demand mismatches exceeding FCAS reserve capacity.

Protection System Manipulation

Altering relay settings or disabling protection systems can prevent automatic isolation of faults, allowing localised issues to cascade system-wide.

Denial of Service on Control Systems

Disrupting communication between grid operators and generators prevents coordinated response, allowing deviations to escalate beyond recovery.

Destructive Malware Deployment

Malware like Industroyer (used in Ukraine) can directly operate circuit breakers while simultaneously wiping control system data, combining immediate disruption with prolonged recovery times.

Optimal Attack Timing

Analysis of NEM operating conditions reveals clear windows of maximum vulnerability to cause a large frequency deviation below 50Hz: During a peak demand period, especially if a key grid element like a large interconnect is not operating, or if a state is operating in island mode.

Season: Summer (December - February)

- Extreme heat drives peak air-conditioning demand
- Highest absolute demand peaks occur on 35°C+ days
- Maximum rooftop solar generation creates steep evening ramp-down

Weather: Heatwave Conditions

- Clear, hot days maximise solar generation (for DER manipulation)
- Sustained heat maintains high demand for air conditioning into evening hours

Time of Day: 12-2 PM

- Solar generation running at peak
- Demand remains near peak from cooling loads
- System transitions to battery/gas backup with lower inertia
- Net demand ramp rates at their steepest

Time of Day: 6-8 PM

- Solar generation downramping to zero as sun sets
- Demand remains near peak from cooling loads
- System transitions to non-solar generation to meet demand

An attack timed to one of these windows could:

- Exploit high DER penetration during early afternoon hours
- Trigger frequency deviations in early evening as solar naturally ramps down
- Overwhelm FCAS reserves already stressed by peak demand
- Cascade into regional or wider blackout before operators can respond

The State of Tasmania is particularly at risk due to interconnect reliability, capacity, and high DER generation in the state. In the 3rd quarter of 2025, for example, Tasmania experienced

96 low frequency excursions outside the normal frequency range without identified contingencies, compared to 0 such events on the mainland section of the NEM.

Attack Scenario Modelling

Potential scenario: Coordinated DER Attack During Summer Peak

Preconditions:

- Mid-February, severe heatwave (40°C+ in Sydney, Melbourne, Adelaide)
- 6:30 PM — solar generation rapidly declining, demand near peak
- System operating normally but with minimal reserves
- Large system facility like interconnect or base load generation offline

Attack Sequence:

T+0 seconds: Attackers activate pre-positioned access across compromised solar inverter platforms, commanding approximately 2 GW of rooftop solar to disconnect simultaneously across NSW and Victoria.
T+2 seconds: Frequency drops from 50.0 Hz to 49.5 Hz. Automatic Generation Control (AGC) responds, calling on FCAS reserves.
T+5 seconds: Attackers command compromised battery systems to switch from discharge to charge mode, adding 500 MW of additional load. Frequency drops to 49.2 Hz.
T+8 seconds: Under-Frequency Load Shedding (UFLS) activates, disconnecting interruptible loads. However, Rate of Change of Frequency (RoCoF) exceeds 3 Hz/second due to low inertia.
T+12 seconds: Frequency passes through 49.0 Hz. Additional generator protection relays trip to prevent equipment damage, removing more supply and accelerating the decline.
T+15 seconds: Frequency reaches 48.0 Hz. NSW-Victoria interconnector separates to prevent cascading into Queensland. South Australia separates from Victoria.
T+20 seconds: Black System event is triggered in Victoria and South Australia. NSW stabilises at degraded capacity with rolling blackouts.
T+30 minutes: Attackers deploy destructive malware across compromised control systems, wiping configuration data and complicating recovery efforts.

Recovery Timeline:

Hours 1-6: Emergency response, damage assessment, initial restoration of critical loads
Hours 6-24: Progressive black start, re-synchronisation of generators
Hours 24-72: Gradual restoration of full supply, continued rolling blackouts in some areas
Days 3-7: Investigation, forensics, hardening before full reconnection

Frequency Deviation Analysis

The 2016 South Australia blackout provides empirical data for frequency collapse dynamics:

- Pre-separation frequency: Above 49 Hz (within contingency band)
- Post-separation nadir: 47-48 Hz (below extreme tolerance)
- Rate of Change of Frequency: ~6 Hz/second
- Time to collapse: 2 minutes from initial network disturbance, less than 1 second from loss of Heywood Interconnector.

In our modelled scenario, coordinated removal of 2-2.5 GW during a 30+ GW demand period represents a ~7-8% sudden supply shortfall — sufficient to overwhelm FCAS reserves (typically 1-2 GW) and trigger uncontrollable deviation.

Research on DER-based attacks indicates that controlling inverters representing just 5-15% of total installed capacity[15] could induce similar cascading failures, depending on:

- Available contingency reserves
- System inertia at time of attack
- Speed and coordination of the attack
- Time of day and seasonal factors

Impact Assessment by Sector

As mentioned earlier, due to the foundational role reliable electricity plays in our modern society, the impact of a grid-level black system has far-reaching consequences across other critical infrastructure.

Telecommunications: Mobile networks fail within 4-8 hours as backup batteries and generators deplete. Fixed-line services may persist longer but depend on exchange power. Coordination of refuelling and system re-start will be complicated by communications infrastructure outages.

Water & Wastewater: Treatment plants have generator backup but may fail during extended outages. Pressure loss in distribution, sewage overflow risks.

Healthcare: Hospitals have backup generation but face medication cold chain breaks, cancelled procedures, diverted ambulances. Home care patients at risk.

Transport: Traffic signals, rail systems, fuel pumps offline. Electric vehicle charging unavailable. Airports may continue with backup power but many flights likely to be grounded as a safety precaution.

Finance: ATMs, EFTPOS, online banking unavailable. Cash economy only, with limited ATM functionality.

Food & Grocery: Refrigeration failure leads to spoilage. Supermarkets close. Food safety concerns within 4-6 hours.

Increasing Grid Resilience

Defending against coordinated cyberattacks on the grid requires action across multiple domains. One key learning from recent cyberattacks such as the December 29, 2025 attack on Poland's DER infrastructure is how critical logging and monitoring is on OT systems. Without these capabilities, it is very difficult to identify what was targeted, what attackers were able to do, and to co-ordinate a rapid recovery.

Technical Measures

1. Strengthen DER Security Standards

- Mandate minimum cybersecurity requirements for grid-connected inverters and batteries
- Require firmware signing and secure update mechanisms
- Establish certification schemes for DER aggregation platforms and VPPs
- Enable remote monitoring by TNSPs, DNSPs and AEMO of DER facilities for anomaly detection

2. Enhance OT Network Segmentation

- Implement defence-in-depth architectures separating IT, OT, and safety systems
- Deploy unidirectional security gateways (data diodes) for critical telemetry
- Eliminate unnecessary connectivity between business networks and control systems
- Regular penetration testing of OT environments by qualified specialists
- Deploy ZTNA (Zero Trust Network Access) to operational environments

3. Improve Visibility and Detection

- Deploy OT-specific intrusion detection systems (IDS) across grid-connected systems participating in the energy market.
- Establish baseline behaviour models for activity on these networks.
- Integrate OT security monitoring with Security Operations Centres (SOCs)
- Share threat intelligence across the energy sector and undertake grid-scale tabletop exercises

4. Harden Control Systems

- Replace end-of-life systems with priority placed on those most likely to be exploited to launch an attack
- Implement multi-factor authentication and monitoring for all remote access
- Establish comprehensive asset inventories including firmware versions
- Develop and test grid-scale incident response playbooks specific to OT environments

5. Continue investing in distributed BESS systems

- While not a cybersecurity control, this measure does improve ability to respond to a frequency deviation event and makes the grid more resilient to disruption.
- Accelerate the opportunity for individuals and organisations to participate in energy markets in order to put more redundancy into grid generation and frequency control

The Path Forward

Preventing this scenario requires concerted action:

For energy market participants:

- Implement robust SOCI Act CIRMP requirements
- Invest in OT security visibility, secure access and incident response capability
- Assess and manage supply chain cyber risks
- Engage qualified specialists for OT security assessment and uplift

For regulators and policymakers:

- Establish minimum security standards for grid-connected DER
- Accelerate transmission investment to improve system redundancy
- Fund research into grid-firming inverters and fast frequency response
- Ensure adequate coordination between energy, cyber, and national security agencies
- Increasing ability to individuals to participate in the energy market, creating a resilient system with millions of generation points that is less vulnerable to grid-level disruption

For the broader community:

- Understand personal resilience requirements for extended outages
- Maintain basic security hygiene on smart home devices
- Support investment in grid modernisation and security

Conclusion

The scenario outlined in this paper - a coordinated cyberattack triggering grid-scale blackout in Australia's National Electricity Market - is not science fiction. The attack vectors exist. The

vulnerabilities are documented. The threat actors have demonstrated both capability and intent.

This scenario is just one of several credible scenarios based on empirical evidence and academic research of nation state-led cyberattacks. Our modelling indicates that an adversary could trigger a significant grid disruption by:

- Compromising the orderly supply of energy to the NEM through attacks on DER, interconnect facilities, or traditional generation capacity.
- Timing the attack for maximum impact - midday or late afternoon during a summer heatwave, when solar generation is either at peak supply or drops rapidly while demand remains near peak
- Overwhelming frequency control reserves with coordinated disconnection or manipulation of distributed resources, faster than automatic protections can respond and pushing frequencies to 47Hz causing cascading blackouts
- Extending recovery time through simultaneous attacks on control systems, wiping configuration data, backup generation, and operational communications
- The result: potential blackout affecting millions of Australians, economic losses in the billions of dollars, and risk to vulnerable lives.

The 2015 and 2016 attacks on Ukraine's power grid proved that cyber operations can directly cause physical disruption to electricity supply. Those attacks were deliberately constrained to demonstrate capability without causing mass casualties. A determined adversary with geopolitical objectives - whether destabilisation, coercion, or preparation for broader conflict - would not exercise such restraint.

The 2024 Iberian power outage demonstrates the increased “runaway train” effect that results from a system without the traditional inertia that comes from base load systems.

Australia's grid transformation creates both opportunity and risk. The shift to distributed, renewable generation improves sustainability and can enhance resilience through diversification. But it also introduces millions of new connected devices, complex control systems, and dependencies on global supply chains that expand the attack surface dramatically. Without a different approach to protect these systems, Australia’s modern grid is more fragile to such a Black Swan event than it could be with some additional investment in the right areas to build resilience, detect indicators of compromise, defend from a live attack scenario, and recover more quickly from a cyberattack.

Reliable access to electricity is such a key part of our modern lives that it is often taken for granted - but this is exactly the fundamental infrastructure that a motivated attacker would target in order to achieve maximum impact, due to the downstream effects a prolonged black system will have on other essential services.

With appropriate investment in security, resilience, and preparedness, we can ensure that when adversaries test our grid, they find it harder to break than expected, and faster to recover than they planned.

Citations

1. ICS Investigation Expert Panel, 2025: Grid Incident in Spain and Portugal on 28 April 2025: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/#Publications_&_Documents
2. Dragos, 2026: ELECTRUM: Cyber Attack on Poland's Electric System 2025: https://hub.dragos.com/report/electrum-targeting-polands-electric-sector
3. CERT Polska, 2026: Energy Sector Incident
4. Report – 29 December: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
5. Critical Infrastructure Security Centre: Security of Critical Infrastructure Act 2018 (SOCI): https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018
6. Department of Home Affairs, 2025: Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules): https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-enhancements-to-cirmp-rules/consultation-paper-proposed-amendments-enhance-cirmp.pdf
7. Oxford Economics Australia, 2025: Data Centre Energy Demand https://www.aemo.com.au/-/media/files/stakeholder_consultation/consultations/nem-consultations/2024/2025-iasr-scenarios/final-docs/oxford-economics-australia-data-centre-energy-consumption-report.pdf
8. Zhong et al., 2020, Impact of Virtual Power Plants on Power System Short-Term Transient Response: http://faraday1.ucd.ie/archive/papers/vppcomm.pdf
9. CISA et al., 2024, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
10. Swan, D, February 2, 2026, *Sydney Morning Herald*, Salt Typhoon hackers ‘almost certainly’ in Australia’s critical infrastructure https://www.smh.com.au/technology/salt-typhoon-hackers-almost-certainly-in-australia-s-critical-infrastructure-20251231-p5nqwn.html
11. FERC, 2021, The February 2021 Cold Weather Outages in Texas and the South Central United States: https://ferc.gov/media/february-2021-cold-weather-outages-texas-and-south-central-united-states-ferc-nerc-and
12. AEMO, 2016, BLACK SYSTEM SOUTH AUSTRALIA 28 SEPTEMBER 2016 https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2017/integrated-final-report-sa-black-system-28-september-2016.pdf
13. Dragos, 2017, CRASHOVERRIDE Analyzing the Threat to Electric Grid Operations: https://nsarchive.gwu.edu/sites/default/files/documents/3869008/Dragos-CRASHOVERRIDE-Analyzing-the-Threat-to.pdf
14. CERC India, 2012, REPORT ON THE GRID DISTURBANCE ON 30TH JULY 2012 AND GRID DISTURBANCE ON 31ST JULY 2012: https://www.cercind.gov.in/2012/orders/Final_Report_Grid_Disturbance.pdf

15. US Department of Energy, 2022, Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid: https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf

Glossary

AEMO - Australian Energy Market Operator. Manages the NEM and wholesale electricity and gas markets.
Black Start - The process of restoring power to a grid after complete collapse, using generators that can start without external electricity supply.
Black Swan - A black swan event is a highly improbable, unpredictable occurrence that carries massive (often catastrophic) consequences and, in hindsight, is frequently rationalized as having been foreseeable or inevitable.
CIRMP - Critical Infrastructure Risk Management Program. Required under SOCI Act for responsible entities managing critical assets.
DER - Distributed Energy Resources. Small-scale generation and storage connected at the distribution level, including rooftop solar, batteries, and EVs.
FCAS - Frequency Control Ancillary Services. Market mechanism for procuring resources to maintain grid frequency stability.
Inertia - The resistance of the grid to frequency changes, provided by the rotating mass of synchronous generators. Low-inertia systems change frequency more rapidly.
NEM - National Electricity Market. The interconnected electricity grid serving Queensland, New South Wales, Victoria, Tasmania, South Australia, and the ACT.
NOFEB - Normal Operating Frequency Excursion Band. The acceptable range for frequency excursions (49.75 - 50.25 Hz) before emergency response activates.
OT - Operational Technology. Hardware and software that monitors and controls physical equipment, including SCADA systems, PLCs, and industrial control systems.
REZ - Renewable Energy Zone. Designated areas for coordinated development of large-scale renewable generation and associated transmission.
RoCoF - Rate of Change of Frequency. How quickly grid frequency changes following a disturbance, measured in Hz/second.
SCADA - Supervisory Control and Data Acquisition. Systems used to monitor and control industrial processes including electricity generation and distribution.
SOCI Act - Security of Critical Infrastructure Act 2018. Australian legislation establishing security obligations for critical infrastructure operators.
SRAS - System Restart Ancillary Services. Contracted capability to restart the grid following a black system event.
UFLS - Under-Frequency Load Shedding. Automatic disconnection of loads when frequency drops below safe thresholds, designed to arrest frequency decline and prevent total collapse.

About NetSeg.io

NetSeg specialises in cybersecurity for Operational Technology environments in Australia. We help organisations build the right programs to identify key OT cyber risks and uplift their OT cybersecurity posture to prevent a cyberattack impacting the safety or production of their OT networks.

Web: netseg.io
Email: leon@netseg.io