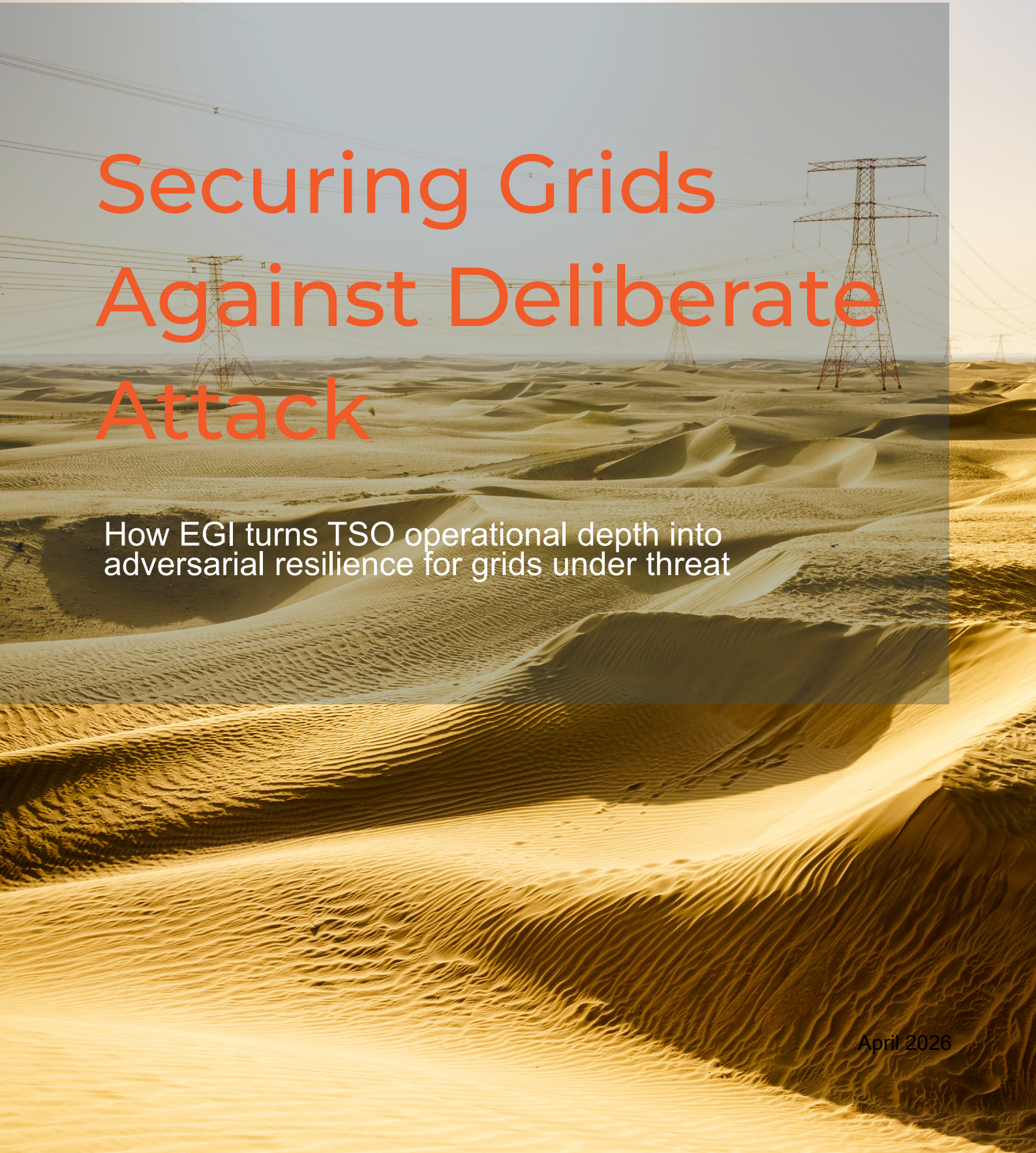
Elia Grid International | STRATEGIC WHITE PAPER

Securing Grids Against Deliberate Attack

How EGI turns TSO operational depth into adversarial resilience for grids under threat



April 2026

Executive Summary

The threat is no longer accidental. It is deliberate.

Power infrastructure is no longer simply a utility asset. It is increasingly exposed to deliberate and targeted disruption, whether physical, cyber, or hybrid in nature. Recent global incidents show that these threats are high-impact, evolving, and not fully addressed by conventional grid planning approaches.

Across regions, electricity systems have been affected by coordinated disruption events, large-scale blackouts driven by cascading failures, and cyber intrusions targeting grid operations. At the same time, growing interconnection has both increased shared vulnerabilities and created new pathways for disruption.

Sector-wide assessments indicate that preparedness remains uneven. Crisis coordination between utilities and national authorities varies, complex scenario exercises are limited, and overall readiness across operators is inconsistent.

For GCC (Gulf Cooperation Council) grid operators, the stakes are particularly high. Power systems underpin essential services such as desalination, cooling, healthcare, and critical national infrastructure. As electrification deepens, the consequences of prolonged disruption continue to increase.

The GCC interconnected grid enhances resilience through shared reserves and cross-border support, but it also introduces dependencies. A disruption affecting a small number of critical nodes can cascade across multiple systems.

The challenge is not effort, but method. Conventional frameworks based on N-1 contingency analysis are designed for random failures, not deliberate disruption. Targeted actions exploit system dependencies and focus on critical asset combinations that can trigger widespread impact—combinations often invisible to standard tools.

What operators cannot see, they cannot protect.

EGI brings the practical operational depth of two active top five European TSOs — Elia Transmission Belgium (ETB) and 50Hertz Transmission Germany — to address this challenge. This paper sets out the nature of that challenge, what makes EGI uniquely positioned to address it, and the evidence from EGI's own project portfolio.

The Problem

When the threat outpaces the plan

Power infrastructure is increasingly exposed to targeted disruption scenarios. Recent global developments show a rise in coordinated incidents affecting energy infrastructure, cyber events impacting grid control systems, catastrophic weather events, and cascading outages across interconnected networks. These developments confirm that disruption can be both deliberate and system-aware, rather than random. These incidents are typically difficult to predict but produce high-impact effects on the power system.

The GCC is not insulated from this reality. Recent regional tensions have made clear that energy infrastructure is no longer just an operational asset. It is a strategic one. A power outage in the Gulf does not simply inconvenience consumers. It threatens desalination plants that supply drinking water, cooling systems that protect human life in extreme heat, medical facilities, and the defense installations that underpin national security. As electrification deepens across the region, the consequences of a targeted, prolonged blackout grow more severe every year.

The GCC interconnected grid, originally built for efficiency, today functions as a regional resilience asset, offering cross-border support, shared reserves, and reduced cascade risk. But interconnection also introduces dependencies. A well-targeted attack on a small number of shared assets or interconnection points can simultaneously degrade multiple national systems. The very integration that strengthens the GCC grid in normal times creates pathways for adversarial exploitation that have not been fully mapped by any member system.

The core problem is structural.

An adversary does not operate according to N-1 logic. They study a system, map its hidden dependencies, and target the minimum combination of assets whose simultaneous loss triggers irreversible cascading collapse.

This combination is the critical cut set.

It is typically invisible within conventional contingency analysis. What operators cannot see, they cannot protect, and they will discover it under the worst possible conditions.

What Current Plans Cover

- Single equipment failures (N-1 criterion)
- Random, independent, probabilistic events
- Natural hazards: storms, floods, heat
- Frequency & voltage deviations
- IT system outages and market suspension

What They Miss — The Adversarial Gap

- Coordinated multi-asset strikes (critical cut sets)
- Targeted attacks designed to exploit dependencies
- Combined cyber + physical hybrid operations
- Missile / drone strikes on substations & transformers
- Cascades engineered to exceed recovery capacity

The danger is not that operators lack protection and contingency planning, it is that their planning frameworks were not designed to anticipate an adversary who studies a system with the specific intent to exploit it.
To close these gaps, a different analytical lens is required that maps system vulnerabilities from the adversary's perspective, before they are discovered under real conditions.

Why EGI?

EGI brings something no other consulting firm can match: an operational foundation built on the live experience of running two of Europe's top five transmission system operators, Elia Transmission Belgium and 50Hertz Germany.

That foundation rests on two pillars. First, real-time operational experience managing highly complex interconnected systems, including system balancing, cross-border coordination, and crisis response. Second, EGI's proven track record of delivering system defense, restoration, and resilience frameworks across diverse system environments.

Elia Grid International brings the crisis management capabilities of Elia and 50Hertz to clients, applying proven frameworks, enforced testing regimes, and validated national exercises to real-world systems.

Proven capability	Elia Transmission Belgium	50Hertz Transmission Germany
System Defense Plan	Published plans that automate actions at crisis start to avoid blackout risk. Updated January 2024 and aligned with EU standards.	Joint plan with German TSOs for coordinated national response. Compliant with Germany's critical infrastructure law since January 2026.
Blackout Restoration	Pre-contracted power plants can restart the grid without external electricity. Self-restart and cross-border recovery tested regularly.	Integrated four-operator recovery framework for all of Germany. No single operator restores the grid alone.
Crisis Management	Government-mandated structure exercised annually with federal and independent authorities through national security exercises.	Emergency protocols with federal agencies. 24/7 monitoring of key systems that control the grid.
Real Incident Record	2006 European Blackout: 15M+ customers affected in 28 seconds. Elia contained the event in Belgium and helped shape ENTSO-E's revised Europe plan.	2012 DDoS cyberattack: A German TSO was targeted and successfully contained the attack with no impact on electricity supply, strengthening cyber threat management across operations.
Cyber & Digital Security	Meets Europe's highest cybersecurity standard for critical infrastructure. Emergency plan covers cyberattacks as operational incidents.	Compliant with Germany's toughest infrastructure law. Dedicated security program for digital control systems of the physical grid.

Our Approach

From Blind Spot to Readiness: EGI's Five-Phase Approach for system resilience

EGI's methodology for system resilience under deliberate threat is structured around five sequential phases, each building on the outputs of the previous. The framework is designed to move an operator from unknown exposure — a system whose critical vulnerabilities have never been mapped through an adversarial lens — to verified, actionable operational preparedness: a system whose operators know where they are most at risk, what the consequences of targeted asset loss would be, and what response actions to execute before they are needed.

The five phases can be entered at any point where a client has existing work to build on, and the scope of each phase can be adjusted to the client's specific system, threat environment, and operational context.

Phase 1

Scope & Threat Alignment

Agree the threat typology and system boundaries relevant to the client's geopolitical and technical context.

Output

- Agreed threat typology
- System boundaries defined
- Data collection framework

Phase 2

Critical Asset Identification

Identify the small asset combinations whose coordinated loss triggers irreversible, system-wide cascading failure.

Output

- Ranked critical cut set register
- Dependency heat map
- Vulnerability priority list

Phase 3

Scenario Development

Build credible physical, cyber and combined attack scenarios calibrated to real system data and threat actor capabilities.

Output

- Validated scenario library
- Scenario-to-consequence mapping
- Attack trees per scenario

Phase 4

Consequence Assessment

Simulate system behavior under each scenario to quantify supply impact, stability effects and recovery bottlenecks.

Output

- Consequence matrix
- Stability analysis results
- Bottleneck identification

Phase 5

Operational Playbooks

Translate findings into pre-defined response sequences that operators can execute under pressure without real-time analysis.

Output

- Operator-ready playbooks
- Coordination protocols
- Exercise scenarios

Proven in the field

Real project experience

EGI's approach is grounded in practical application. Its experience spans system defense planning, restoration strategy, operational readiness, and incident response across multiple regions.

NORTH AFRICA, NATIONAL TSO

Blackout Restoration Strategy & Full Defense Plan

Complete rebuilding of a national TSO's system defense schemes, operational procedures, and Emergency Management & Restoration Plan. Included N-1/N-k contingency analysis, dynamic stability modelling, UFLS/UVLS scheme design, and full operator training.

CONTINENTAL EUROPE — REAL INCIDENT (2006)

European Blackout: Defense Plan Activation & Response

During a Europe-wide blackout affecting 15M+ customers in 28 seconds, Elia contained the Belgian impact (e.g. Antwerp, Ghent, Liège) and restored full grid synchronization in 38 minutes — real operational experience that informed ENTSO-E's subsequent guideline revision.

BELGIUM — PARENT TSO (LIVE OPERATION)

System Integrity Protection Scheme (SIPS) Offshore Corridor

Elia designed and operated a live SIPS for Belgium's 2,000 MW offshore wind/HVDC corridor protecting against blackout/brownout contingencies identified through EMT analysis. This is real critical cut set analysis, operationalized as a live protection scheme.

MIDDLE EAST & GULF — 20+ COUNTRIES

System Operation, Grid Code & Resilience Advisory

EGI has delivered system operation, grid code development, and resilience advisory across the Gulf and wider Middle East — working within the specific system architectures and regulatory cultures of the region.

EASTERN EUROPE — NATIONAL TSO

Dispatcher Training & Emergency Operations Assessment

Assessed TSO's operational readiness for emergency conditions and designed a bespoke dispatcher simulator program modelled on Elia's own crisis training architecture — building the human response capacity that determines recovery speed under pressure.

Discover more projects that we delivered on our website

What We Offer

A consistent finding across resilience assessments is that technical capability alone is insufficient. System performance under stress depends on organizational readiness, decision-making structures, and coordination mechanisms.

EGI builds on crisis management frameworks developed and tested within European TSO environments. These include structured crisis scenario organizations, defined escalation and decision processes, and regular large-scale exercises involving national authorities. They also include integrated approaches to cyber and operational incident response.

These frameworks are adapted to client environments, ensuring that they are both robust and practical. The objective is not only to design systems that can withstand disruption, but to ensure that organizations can respond effectively when disruption occurs.

Core Deliverables

Clear Visibility into System Vulnerabilities

A ranked register of critical asset combinations, quantified by consequence and prioritized by exposure, so protection and investment decisions align to real adversarial risk, not generic standards.

Validated Adversarial Scenario Library

A set of physically consistent threat scenarios, physical, cyber, and hybrid, developed in collaboration with the client's operators and calibrated to their real system data, providing a permanent resource for ongoing planning and exercise.

Operational Playbooks

Pre-defined decision sequences executable under pressure, without real-time analysis during a crisis, integrated into existing emergency plan structures.

Exercise Program

Structured tabletop and operational exercises that stress-test playbooks, identify gaps in decision chains, and build the institutional readiness that determines whether response is effective when it is needed.

EGI transfers this proven crisis management architecture to clients through robust frameworks, tested processes, and exercise programs developed in coordination with national authorities, adapted to your system and your organization.

Conclusion

Resilience depends on identifying the few combinations of assets that can bring the system down

Power systems in the Middle East are operating in a threat environment that has fundamentally shifted. Deliberate attacks, coordinated physical strikes, cyber intrusions, and hybrid scenarios now represent a credible and active risk that conventional N-1 planning frameworks were never designed to address. An adaptive adversary will target the smallest combination of assets whose loss triggers cascading collapse. These critical cut sets are typically unknown to operators, and that blind spot is where exposure remains.

Most utilities have already invested in physical security and emergency response. The gap is not one of effort, but of visibility. Existing frameworks do not account for adversarial logic, and without that perspective, the most critical vulnerabilities remain hidden until they are exposed under real conditions.

Closing this gap requires a shift from reactive protection to proactive identification. Operators need to know which assets matter most, which combinations create system-level risk, and how the system will behave under targeted disruption. Just as importantly, they need clearly defined operational responses that can be executed under pressure.

For operators, this creates a clear opportunity to strengthen resilience in a targeted and efficient way. For regulators and ministries, it provides a structured basis to manage cross-border dependencies and reduce the risk of regional escalation. For security stakeholders, the missing link is not threat intelligence, but its translation into physically consistent system behaviour.

EGI supports this transition. Through direct engagement with regional systems and the operational experience of its parent TSOs, Elia and 50Hertz, EGI brings verified network knowledge rather than approximations from public data. Its five-phase methodology moves from critical asset identification to threat scenario modelling, consequence assessment, and operational response design within a single consistent framework.

The outcome is practical and immediate. Operators gain clear visibility on their most critical vulnerabilities, prioritised actions, and operational playbooks that can be implemented without additional capital investment.

About Elia Grid International

Elia Grid International (EGI) is a leading consultancy specializing in addressing complex power system challenges. Drawing expertise and innovative solutions from two of Europe's top transmission system operators, EGI delivers strategic, technical, and regulatory guidance across all aspects of power transmission.

Over the past 10 years, EGI has grown into a truly global player, built on a fantastic human journey. What started as a team of 10 experts who broke a new strategic ground to establish a consulting company has evolved into a trusted partner worldwide.

Today, EGI has successfully delivered more than 320 projects in over 20 countries, extending its reach across all seven continents.

Are you ready to partner with us?

eliagrid-int.com