Baringa

Securing Germany’s energy networks against nation state threats

E World 2026

A snapshot of Baringa

A globally leading advisory business helping organisations navigate the energy transition

Who we are

2000+ People

6 Industry sectors

1000+ Energy experts

400+ Energy clients

60+ Countries where we model the energy system

TOP 10 Great places to work

Putting people first.
Creating impact that lasts.

What we do

Analyze and design markets and policy

Determine strategy and investment decisions

Identify new commercial opportunities and manage risk

Structure and run more effective businesses

All underpinned by a world leading energy market modelling capability

FT FINANCIAL TIMES statista UK'S LEADING MANAGEMENT CONSULTANTS 2018 – 2025

BEST OF CONSULTING 2020 RISIKO MANAGEMENT 4. PLATZ Baringa Partners LLP Wirtschafts Woche

Beste Arbeitgeber Consulting Great Place To Work. Deutschland 2025

Beste Arbeitgeber NRW Great Place To Work. Deutschland 2021

Beste Arbeitgeber kleiner Mittelstand Great Place To Work. Deutschland 2021

Best Workplaces in Consulting & Professional Services Great Place To Work. UK 2025

Best Workplaces for Women Great Place To Work. UK 2025

Best Workplaces for Wellbeing Great Place To Work. UK 2025

Forbes WORLD'S BEST MANAGEMENT CONSULTING FIRMS POWERED BY statista 2025

Great Place To Work. Certified OCT 2023-OCT 2024 UK

BUSINESS IN THE COMMUNITY The Prince's Responsible Business Network Race at Work Charter signatory

THE UK'S 100 BEST LARGE COMPANIES TO WORK FOR 2021

Baringa

On a cold February day, all power grids in Europe collapsed. A total Blackout.

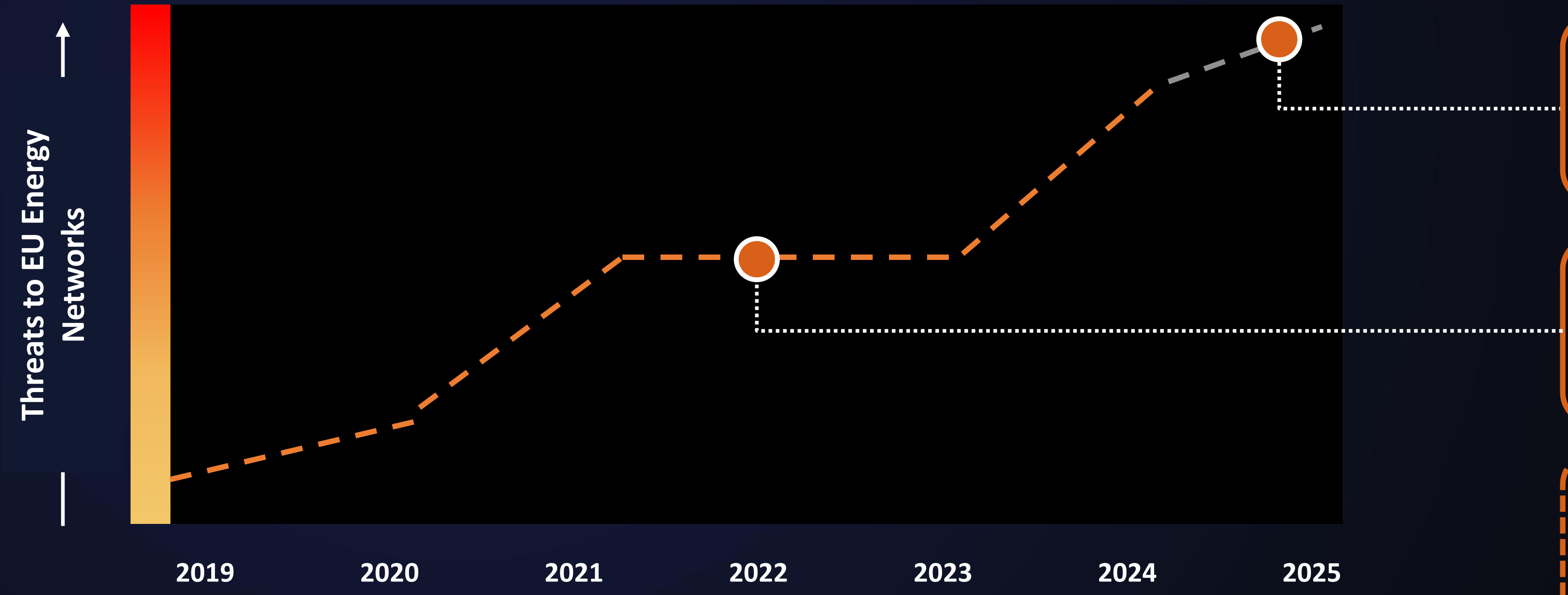
Novel: Blackout by Marc Elsberg, 2012

The threat of cyber attacks disrupting Germany's energy networks is intensifying

Nation states	
Capability	5/5
Intent	3/5

Cyber criminals	
Capability	3/5
Intent	3/5

Hacktivists	
Capability	3/5
Intent	3/5



Polish DER Cyber Attack
2025

German Wind Sector Cyber Attacks
2022

Berlin Power Outage
2026

Baringa

The rising threat to Germany’s energy networks is driven largely by geopolitical instability, easier access to sophisticated cyber attack capabilities through AI, and greater network digitalisation

Geopolitics

Digitalisation

Lower bar to entry

In a tense geopolitical climate, Germany’s energy infrastructure is a strategic target

Geopolitics

Nation state capability is already mature.

The real variable is intent, and foreseeable **geopolitical flashpoints** could quickly raise it, accelerating both the volume and severity of state-linked attacks.

Germany is a strategic target, not just a victim of opportunity:

- ✓ **Europe’s largest economy**
- ✓ **A central energy hub**
- ✓ **A key political and military actor in NATO and the EU**

Digitalisation

Lower bar to entry

AI and cybercrime-as-a-service have erased the skill gap, enabling threat actors to operate with high capability and vastly expanding the pool of attackers

Lower bar to entry

As the increased accessibility of advanced techniques commoditises cybercrime, sophisticated capability is no longer the constraint – **intent and opportunity** now drive the scale and impact of attacks.

States increasingly leverage or tolerate criminal and hacktivist proxies, blurring attribution and preserving deniability.

With the barrier to entry dramatically lowered, the pool of capable attackers expands, resulting in **more actors, more attacks and heightened systemic risk** to Germany’s energy networks.

Geopolitics

Digitalisation

The increasing Digitalisation through Smart Meters – intelligent Metering Systems – increases cyber risk

Geopolitics

Lower bar to entry

Digitalisation

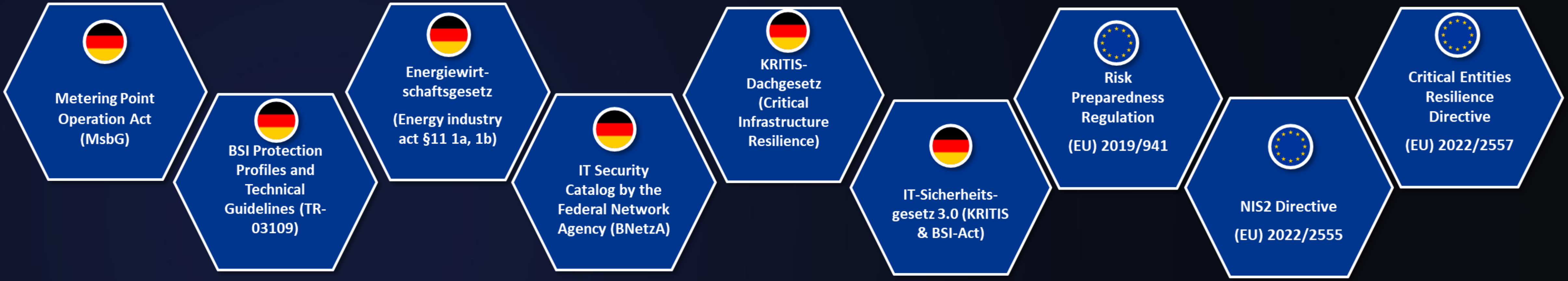
Expanded Attack Surface
Massive deployment, IoT connectivity

Remote Control and Automation
Remote commands, Firmware updates

Sensitive Data Exposure
Consumption data, data in transit/at rest

Increased Complexity and Decentralisation
Integration Smart Grid, Third parties

Understanding and meeting regulatory requirements provides the foundation for a more comprehensive and resilient cyber-posture



- Metering Point Operation Act (MsbG)
- BSI Protection Profiles and Technical Guidelines (TR-03109)
- Energiewirtschaftsgesetz (Energy industry act §11 1a, 1b)
- IT Security Catalog by the Federal Network Agency (BNetzA)
- KRITIS-Dachgesetz (Critical Infrastructure Resilience)
- IT-Sicherheitsgesetz 3.0 (KRITIS & BSI-Act)
- Risk Preparedness Regulation (EU) 2019/941
- NIS2 Directive (EU) 2022/2555
- Critical Entities Resilience Directive (EU) 2022/2557

Furthermore, there are three priority areas where Germany's network operators must focus on to tackle current and future threats:

- Managing the hybrid threat & risk landscape
- Building resilience to cyber attacks
- Securing digitalisation by design

Hybrid risk management is essential because cyber and physical intrusions can mutually enable high-impact disruption

Managing the hybrid threat & risk landscape

Building resilience to cyber attacks

Securing digitalisation by design

Understand who the adversaries are, what they can do, and what they are targeting. Translate this into an understanding of the potential impact on your end-to-end energy system, recognising that attackers do not respect organisational or technical silos and will exploit gaps between IT, OT and physical operations.

- ✓ Actively manage the seams between IT, OT and operational silos common in Germany’s integrated utilities
- ✓ Create end-to-end cyber-physical risk view and prioritise based on system criticality, not asset count
- ✓ Anchor risk-based decisions in real-world impact (safety, availability, grid stability)
- ✓ Conduct joint scenario planning across IT, OT, security and operations

The ability to continue operations, recover quickly and limit cascading outages is critical to national stability and public trust

Managing the hybrid threat & risk landscape

Building resilience to cyber attacks

Securing digitalisation by design

In the context of Germany’s energy threat landscape, it is best to prepare for ‘when’ not ‘if’ cyber attacks happen. It is not possible to prevent every attack, so it is critical to be able to ensure continuity of supply and rapid recovery when disruption occurs, and learn from it.

- ✓ Detect, contain and recover – not just prevent
- ✓ Coordinate and exercise response across IT, OT and operations – build muscle memory in your teams and identify weaknesses before the real-life event
- ✓ Ensure leadership ownership of cyber crisis response and decision making
- ✓ Embed cyber into holistic resilience to tackle the increasingly interconnected and complex energy sector risk landscape

Securing digitalisation by design ensures a resilient energy transition and new digital capabilities do not create systemic risk

Managing the hybrid threat & risk landscape

Building resilience to cyber attacks

Securing digitalisation by design

Digitalisation is not the risk, but unsecured and unmanaged digitalisation is. As Germany's energy system becomes more digitalised, connected and decentralised, security must be built in by design, governed at a strategic level, and embedded across the asset lifecycle to ensure resilience.

- ✓ Embed security and resilience into OT modernisation, cloud adoption and smart metering systems
- ✓ Assign clear risk ownership for new digital initiatives
- ✓ Make architecture decisions with failure scenarios in mind
- ✓ Treat suppliers, service providers and digital ecosystems as part of the interconnected threat model

„Energy security is a central pillar in the German security architecture… The energy sector is particularly in focus for state-supported operations, cybercriminals, who blackmail energy companies or pursue ideological goals.“

BSI, 2025

Contact

Isabelle Sheard

Manager
Digital Risk & Cyber
Phone: +44 7540 108193
Email: isabelle.sheard@baringa.com

Ralf Kurtz

Director
Energy & Resources
Phone: +49 175 4328050
Email: ralf.kurtz@baringa.com

Please don’t hesitate to contact us!