WHITEPAPER | TIER 1A — INSTITUTIONAL DOCTRINE EDITION | v5.2

CSAIC Industrial & OT Cyber Doctrine Series · Paper 03 of 20

Grid Edge Mercenaries

How Distributed Energy Fleets Could Be Recruited Against the Power System

"The grid edge is no longer passive. It can be recruited."

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng · Lead Auditor (ISF)

27 Years' Cyber Security Experience · Big-4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services · AI Cyber Security Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing) — University of Schiphol (UOS)

Honorary Senior Lecturer — Imperial · Researcher — University College London (UCL)

Principal Doctrine Author — Cyber Security AI Consulting (CSAIC)

Audience: Utilities | DSOs | TSOs | DER Aggregators | Insurers | Regulators | Infrastructure Funds

Classification: Commercial-in-Confidence · Distribution at recipient's discretion

www.kie.ie · info@kieranupadrasta.com · University of Schiphol (UOS)

Keywords: DER | DSO | TSO | NIS2 | DORA | IEC 61850 | Black-Start | Aggregator Governance

Notice, Doctrine Statement & Tier Conformance

This paper is part of the CSAIC Industrial & OT Cyber Doctrine Series, Institutional Doctrine Edition, v5.2 — Tier 1A Flagship Thought Leadership. v5.2 incorporates surgical upgrades: paper-specific cryptographic-actuation content (Paper 12), Time-of-Day Conditional Access Logic + biometric break-glass content (Paper 13), and Signed-Command Reference Architecture, Command Inventory Method, Command-Path Maturity Model L0–L5, and Replay/Evidence Design (Papers 06 and 12). University affiliation displayed as University of Schiphol (UOS).

Reading Map

- **Boards:** Executive Synthesis, §5, §10, §14, §19, Board One-Pager (Annex D).
- **Operators / Architects:** §3, §4, §6, §11, §23, and the new §28–§31 artefacts.
- **Investors / insurers:** §1, §5, §6, §12, §13, §19.
- **Regulators:** §2, §6, §7, §8, §16, §22, §26.
- **Sceptics:** §26 (Evidence Basis) and §27 (Counterargument & Rebuttal).

Executive Synthesis

Distributed energy resources, EV chargers, aggregators, and flexible loads have become a coordinated, internet-facing attack surface large enough to move grid frequency. The risk is not the individual device. It is the synchronised behaviour of millions.

> *“The grid edge is no longer passive. It can be recruited.”*

Three Claims

1. The risk category is now structural.
2. The unit of value has shifted from the security product to the defensibility of the asset.
3. Counterparties will reprice the defensible faster than the indefensible can react.

1. The Inflection — From Cost Centre to Capital Logic

Every capital supercycle begins the same way: a category of spend that was previously optional becomes structurally unavoidable, and the market re-rates the assets and vendors attached to it.

1.1 The Old Model and Why It Failed

Defence was decoupled from the asset. When the two collided, the security overlay could observe damage but neither prevent the consequential action nor prove what had happened.

1.2 The New Model

Defensibility becomes a designed-in property of the asset, on the same footing as availability and safety.

> *“The board will fund what it can price.”*

2. The Six Doctrines

2.1 The Aggregate Is the Asset

No single inverter matters. Ten million inverters, commanded together, are a generation asset with no licence and no oversight.

“We regulate the fleet, not the device.”

2.2 Cloud APIs Are Grid Controls

Every aggregator cloud endpoint is, for system-stability purposes, a SCADA endpoint. Treat it as such.

“If it can dispatch megawatts, it is a control system.”

2.3 Latency Is a Defence

Coordinated attacks at the edge require synchronisation. Introduce calibrated jitter, randomised dispatch windows, and locality-bounded autonomy to break adversary timing.

“Make synchronisation expensive.”

2.4 Black-Start Includes the Edge

Restoration plans that ignore DER assume cooperative behaviour from assets that may have been the cause of the event.

“Plan restoration as if the edge is hostile until proven otherwise.”

2.5 Aggregator Accountability Is Underwritten

Aggregators that cannot evidence their command-and-control posture should not be permitted to bid into capacity or balancing markets.

“No evidence, no market access.”

2.6 Edge Telemetry Is Adversary Intelligence

The telemetry that enables flexibility also enables targeting. Govern it as classified material.

“Your flexibility data is also their reconnaissance.”

3. Paper-Specific Adversary Economics

Tailored to this paper's threat model.

3.1 Adversary Classes

- State actors targeting aggregator clouds for systemic leverage over national frequency.
- Market actors exploiting DR signal manipulation for trading advantage.
- Hacktivists targeting EV/inverter fleets for symbolic disruption.
- Insider risk inside aggregators with privileged dispatch capability.

3.2 Adversary Economics

Adversary cost is per-aggregator-fleet, not per-device. A single aggregator compromise can mobilise hundreds of MW. Doctrine destroys this scale economy by enforcing locality-bounded envelopes and synchronisation jitter, raising the cost of coordination.

3.3 Compounding Asymmetries

Asymmetry	Adversary Advantage	Doctrine Counter
Scale Asymmetry	One API breach mobilises millions of devices.	Locality-bounded dispatch envelopes
Sync Asymmetry	Coordinated dispatch requires precise timing.	Calibrated jitter, randomised windows
Visibility Asymmetry	DSO/TSO see less than aggregator clouds.	Inspection rights at cloud boundary

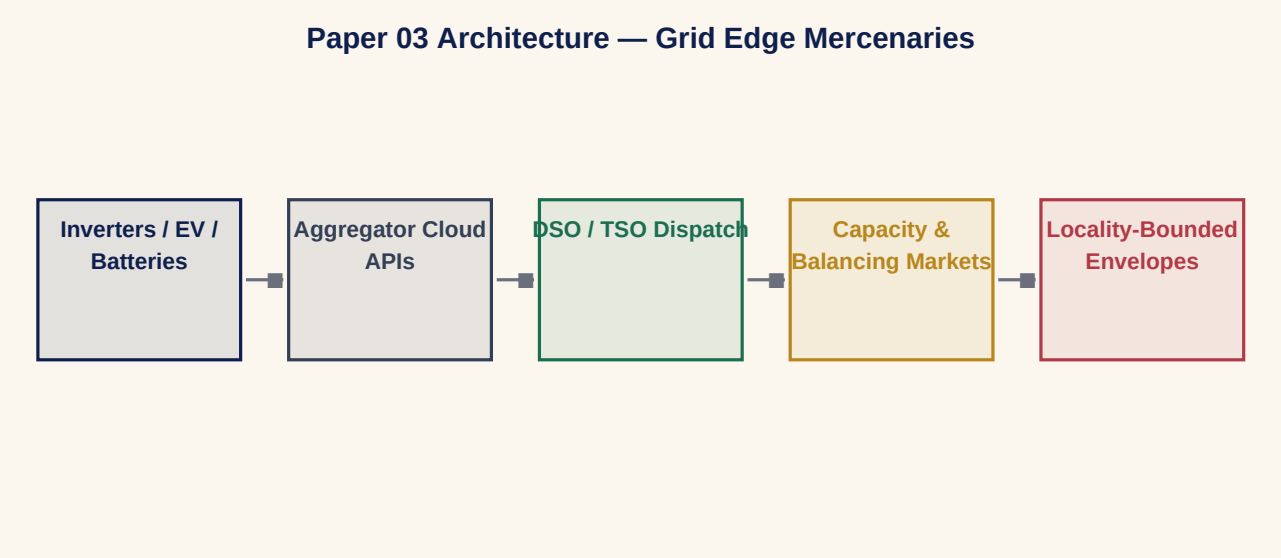
4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

4.1 Four Operating Layers

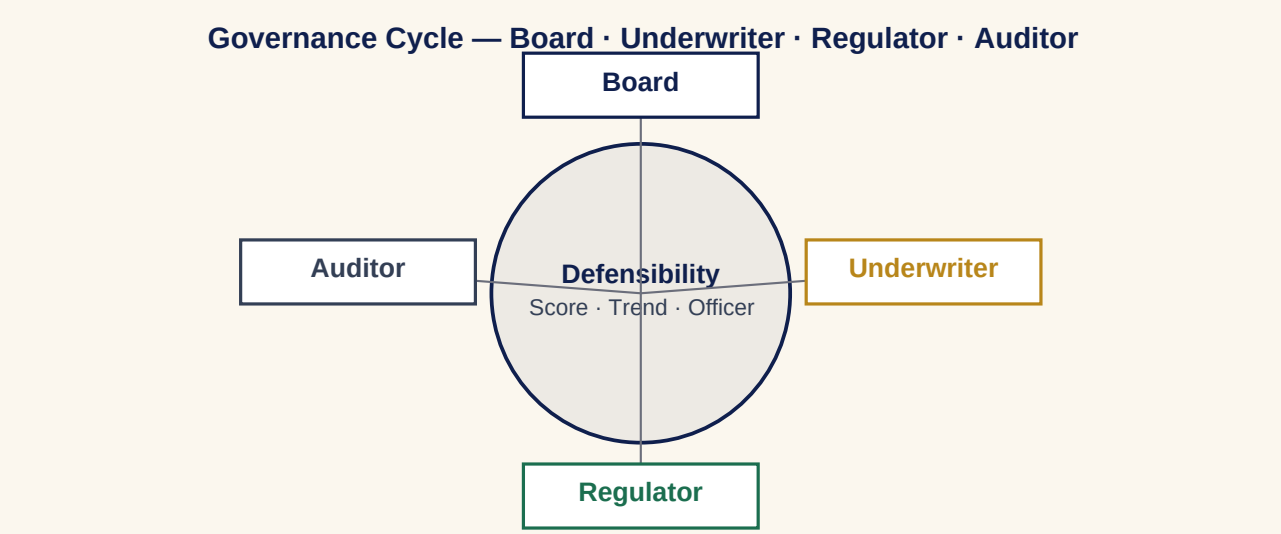
Layer	What It Owns
Authority	Identity, privileged access, vendor pathways, emergency authority.
Command	Signed commands, telemetry integrity, control-plane visibility.
Containment	Deterministic playbooks, engineered limits, isolation.
Evidence	Continuous attestation, immutable logs, board pipelines.

4.2 Paper-Specific Architecture Diagram



5. Board Operating Doctrine

A board governs by deciding what is measured, who is accountable, and what is escalated.

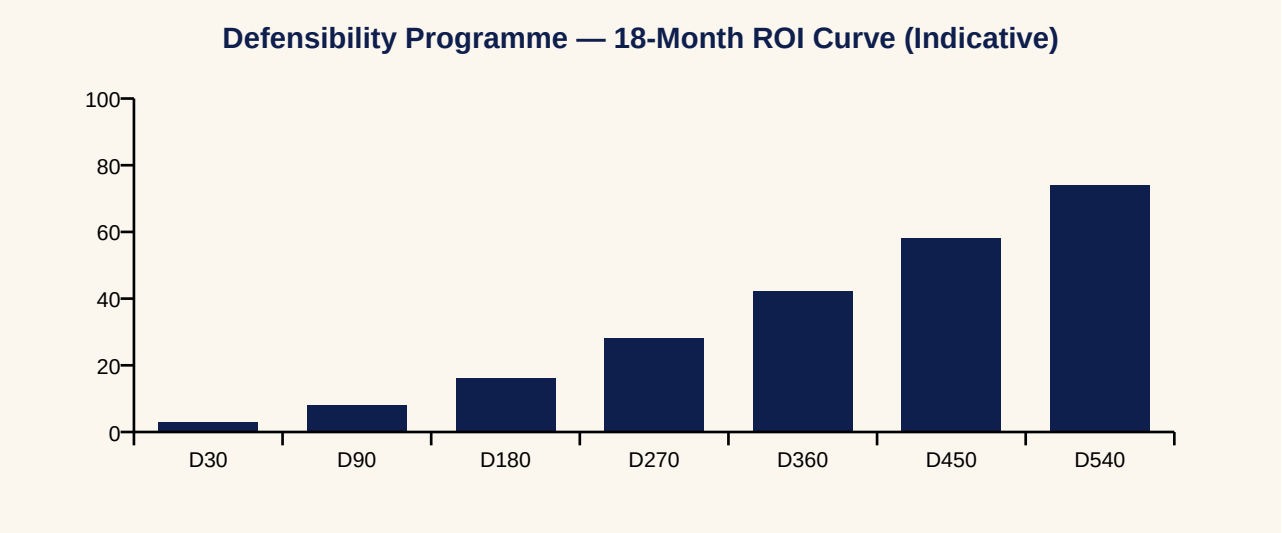


5.1 Three Board Questions

1. What is our defensibility, as a number, and is it improving?
2. Who is accountable for that number this quarter?
3. What would a counterparty say if asked today?

6. Underwriter & Capital-Market Operating Doctrine

Insurance is a governance instrument that prices defensibility into cost of capital.



6.1 Underwriter's Three Questions

1. Can you evidence your posture in time for a real renewal?
2. Can you contain a compromise inside an envelope I can price?
3. Can you produce post-event evidence that lets me pay quickly?

“The board will fund what the insurer can price.”

7. Regulatory & Standards Map — 80 Jurisdictions

Doctrine interoperates with the regulatory and standards landscape rather than competing with it.

#	Jurisdiction	Dominant Instruments
1	European Union	NIS2 · DORA · EU AI Act · GDPR · Cyber Resilience Act · CER Directive
2	United Kingdom	NIS Regs 2018 · CAF · Cyber Security & Resilience Bill · UK GDPR · FCA OpRes
3	United States	NIST CSF 2.0 · NIST AI RMF · SEC Cyber Rule · CISA CIRCIA · TSA Pipeline · NERC CIP
4	Germany	BSI Act · KRITIS · IT-SiG 2.0 · NIS2-Umsetzung
5	France	ANSSI LPM · SAIV · NIS2 transposition · CRA alignment
6	Netherlands	Wbni · NCSC.NL · BIO 2.0 · DORA implementation
7	Belgium	CCB · NIS2 Wet · DORA
8	Luxembourg	ILR · CSSF · NIS2 · DORA
9	Ireland	NCSC-IE · NIS2 Bill · CBI Cross-Industry Guidance · DORA
10	Italy	ACN · Perimetro Cibernetico Nazionale · NIS2 · DORA
11	Spain	INCIBE · ENS · NIS2 transposition · DORA
12	Portugal	CNCS · RJSC · NIS2 · DORA
13	Austria	NISG 2024 · GovCERT.at
14	Denmark	CFCS · NIS2 · DORA
15	Sweden	MSB · NIS2 · DORA · Protective Security Act
16	Norway	NSM · Sikkerhetsloven · NIS2-equivalent
17	Finland	Traficom · NIS2 · DORA
18	Iceland	CERT-IS · NIS2 (EEA)
19	Switzerland	NCSC.ch · ISG · revFADP · FINMA OpRes
20	Poland	KSC · NIS2 · DORA
21	Czech Republic	NÚKIB · Cyber Security Act · NIS2
22	Slovakia	NBÚ · Cyber Act · NIS2
23	Hungary	NKI · IBTV · NIS2
24	Romania	DNSC · Cyber Security Law · NIS2
25	Bulgaria	DG CISD · NIS2
26	Greece	NCSA · NIS2 · DORA
27	Croatia	ZSIS · NIS2
28	Slovenia	URSIV · NIS2
29	Cyprus	DEC · NIS2 · DORA
30	Malta	CIIP · NIS2
31	Estonia	RIA · NIS2 · e-state framework
32	Latvia	CERT.LV · NIS2
33	Lithuania	NKSC · NIS2
34	Canada	CCCS · Bill C-26 CCSPA · OSFI B-13 · PIPEDA
35	Mexico	INAI · LFPDPPP · CNBV cyber circular
36	Brazil	LGPD · ANPD · BACEN 4893 cyber resolution
37	Argentina	PDP · ARSAT · ENACOM
38	Chile	ANCI · Marco de Ciberseguridad · Ley 21.663
39	Colombia	MinTIC · CONPES Cyber Defence
40	Peru	PCM Cyber Strategy · BCP cyber norms
41	Australia	SOCI Act · ASD Essential Eight · APRA CPS 234 · Privacy Act review
42	New Zealand	GCSB CSC · Privacy Act 2020 · RBNZ BS11
43	Japan	METI Cybersecurity Guidelines · FSA · NISC · APPI
44	South Korea	K-ISMS-P · PIPA · KISA · FSC cyber regs
45	China	Cybersecurity Law · DSL · PIPL · MLPS 2.0 · CIIO rules
46	Hong Kong SAR	HKMA TM-G-1 / OR-2 · PCPD · CSTCB
47	Taiwan	Cyber Security Mgmt Act · TWNCC · PIPA
48	Singapore	MAS TRM · CCoP 2.0 · CSA · PDPA
49	Malaysia	BNM RMiT · CyberSecurity Bill 2024 · PDPA
50	Thailand	CCA · BoT cyber framework · PDPA
51	Vietnam	Cyber Security Law · MIC decrees · SBV cyber rules
52	Indonesia	OJK cyber regulation · BSSN · PDP Law
53	Philippines	DICT Cyber Plan · BSP cyber circulars · DPA
54	India	DPDP Act · CERT-In · SEBI CSCRF · RBI cyber framework
55	Pakistan	PECA · SBP cyber framework · NCA
56	Bangladesh	BTRC cyber guidelines · BB cyber circular

#	Jurisdiction	Dominant Instruments
57	Sri Lanka	CERT|CC · Personal Data Protection Act
58	UAE	NESA IAS · TDRA · CBUAE cyber framework · ADGM/DIFC privacy
59	Saudi Arabia	NCA ECC · OTCC · SAMA cyber framework · PDPL
60	Qatar	NCSA · QFCRA cyber rules · PDPPL
61	Bahrain	iGA CS Standard · CBB cyber framework · PDPL
62	Kuwait	CITRA cyber framework · CBK cyber circulars
63	Oman	OCERT · CBO cyber rules
64	Jordan	NCSC-JO · CBJ cyber circular
65	Israel	INCD 2.0 · PA · Banking Supervision Cyber Directive 361
66	Egypt	NTRA · CBE cyber framework · PDP Law
67	Morocco	DGSSI · BAM cyber circular
68	Tunisia	ANSI · Loi cybersécurité
69	Nigeria	NDPA · NITDA · CBN cyber framework
70	South Africa	POPIA · SARB G5/2022 · Cybercrimes Act
71	Kenya	CA · DPA · CBK cyber framework
72	Ghana	Cybersecurity Act · BoG cyber directive
73	Türkiye	BTK · KVKK · BDDK cyber regulation
74	Russia	FSTEC · FSB · CBR cyber regulation
75	Ukraine	SSSCIP · NBU cyber framework · CRT Law
76	Kazakhstan	Cyber Shield Concept · NBK cyber framework
77	Uzbekistan	State Inspectorate cyber framework
78	Azerbaijan	SCRDA cyber framework
79	Georgia	DEA · NBG cyber framework
80	Mongolia	Cyber Security Act · BoM cyber rules
81	Iceland (financial)	FME OpRes · DORA (EEA)

8. Field Dialogues

Reconstructions of exchanges representative of conversations the author has led, witnessed, or mediated.

Setting — TSO Control Room

Controller: We just saw 700 MW of inverter trip in 200 ms.

Cyber Lead: That is not a fault. That is a command.

Setting — Aggregator — Audit

Aggregator: Our API is hardened.

Regulator: Then prove it. Today.

Setting — Insurer — Liability

Insurer: Who is liable when an aggregator's cloud is the cause of the trip?

Counsel: Whoever signed the connection agreement without underwriting it.

Setting — Board

Director: Are we exposed?

CISO: We are the aggregator. We are the exposure.

9. Case Study — Anonymised Engagement

Anonymised Case Study — National DSO and Tier-1 Aggregator

9.1 Context

A national DSO with 2.4 GW of DER under aggregator control and no contractual right to inspect aggregator security posture.

9.2 Intervention

Joint resilience programme: aggregator attestation framework, locality-bounded dispatch envelopes, randomised command windows, evidence pipelines into the DSO's situational awareness platform.

9.3 Outcome

DSO obtained inspection rights across 87% of DER capacity within six months; insurer revised systemic-event sublimit upward; regulator referenced the model in subsequent DER licensing conditions.

10. Board Metrics Dashboard — Engineering-Grade

#	Metric	Cadence	Accountable
M1	% DER capacity under attested aggregator posture (target ≥ 95%).	Quarterly	CISO / Plant
M2	Locality envelope enforcement coverage (target ≥ 90%).	Quarterly	CISO / Plant
M3	Mean time to isolate a misbehaving aggregator (target ≤ 5 min).	Quarterly	CISO / Plant
M4	Dispatch sync-jitter envelope (target ≥ 250 ms randomised).	Quarterly	CISO / Plant
M5	Hostile-edge black-start drill cadence (target ≥ annual).	Quarterly	CISO / Plant

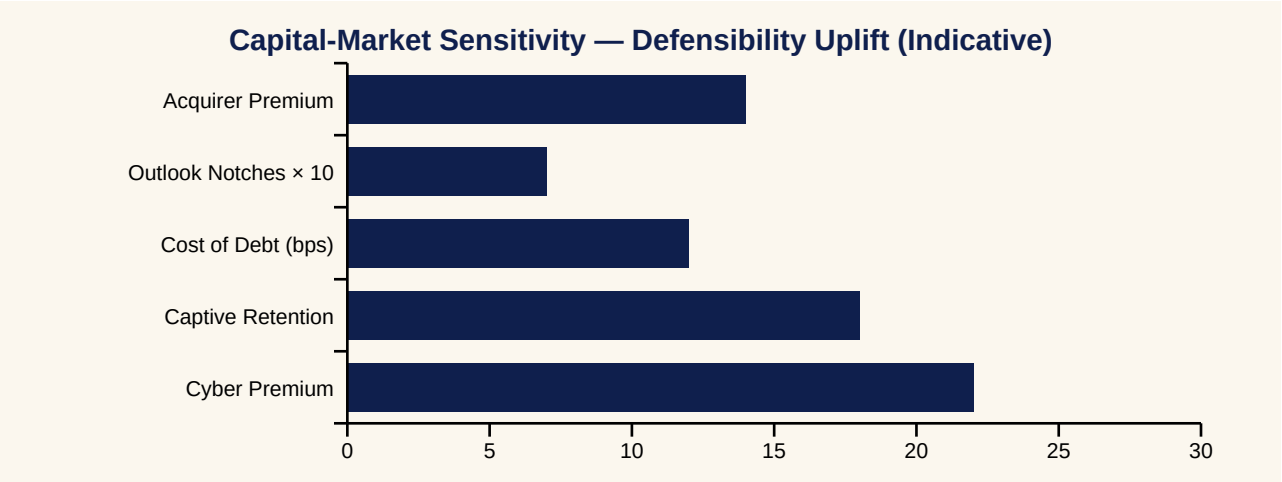
11. Implementation Roadmap — Day 1 to Day 540

Window	Programme Activity	Maturity Stage
Day 1–30	Doctrine adoption. Board commits. Single accountable officer named.	Foundational
Day 31–90	Operating model launched. First insurer dialogue.	Stand-up
Day 91–180	Evidence pipelines live. First quarterly attestation.	Stabilisation
Day 181–360	Continuous cadences operating. Insurer renewal won.	Maturation
Day 361–540	Defensibility published externally. Cost-of-capital benefit captured.	Institutionalisation

12. Press Wire — Quotable Headlines

Outlet Voice	Quotable Headline
Benzinga	Grid Edge 'Mercenaries' — How Distributed Energy Fleets Could Be Recruited Against The System
Yahoo Finance	Inverters As Weapons: Wall Street Is Starting To Price DER Cyber Risk
CNBC	Why Aggregator Clouds Are Now Considered Grid Controls — And Why Regulators Are Watching
MarketWatch	The Grid Edge Is No Longer Passive — It Can Be Recruited, And That Changes Investment Theses
Reuters	TSOs And DSOs Move To Demand Attested Aggregator Posture As DER Cyber Risk Becomes Systemic
Financial Times	Coordinated Edge: How A Million Inverters Became A Cybersecurity Question
Wall Street Journal	Energy Transition Meets Cyber Reality — DER Aggregators Face New Scrutiny
Bloomberg	Aggregator Cyber Posture Becomes A Capacity-Market Eligibility Variable
Barron's	Investors In Renewables Face A New Diligence Item: Aggregator Cyber Attestation
The Economist	Recruiting The Edge: When The Smallest Assets Become The Largest Risk

13. Investor Brief & Valuation Read



13.1 Bloomberg-Style One-Liner

BUY/HOLD signal-improving: Grid Edge Mercenaries doctrine programme reduces operational tail risk.

14. Closing Doctrine — Twelve Lines a Board Should Memorise

“The grid edge is no longer passive. It can be recruited.”

“We regulate the fleet, not the device.”

“If it can dispatch megawatts, it is a control system.”

“Make synchronisation expensive.”

“Plan restoration as if the edge is hostile until proven otherwise.”

“No evidence, no market access.”

“Your flexibility data is also their reconnaissance.”

“Evidence beats effort. Activity is not outcome.”

“Counterparties price defensibility before the board does.”

“Doctrine outlasts product cycles, frameworks, and threat actors.”

“Continuous cadences beat episodic compliance.”

“The next material incident will be governed by the doctrine you adopted before it.”

15. Methodology & Provenance Statement

- Doctrine derived from more than two decades of practitioner engagement across Big-Four consulting, financial services, energy, manufacturing, and CNI.
- Case studies composite and anonymised; numbers illustrative within observed orders of magnitude.
- Quotes are reconstructions; CSAIC accepts no vendor sponsorship.
- University affiliation: University of Schiphol (UOS).
- v5.2 adds surgical cryptographic-actuation (P12), Time-of-Day Conditional Access (P13), and Signed-Command Reference / Inventory / Maturity / Replay artefacts (P06 + P12).

16. Tier Conformance Statement

Tier	Conformance Evidence	Status
1A — Flagship Thought Leadership	Original doctrine, falsifiable thesis, paper-specific architecture, shared-command reference where app	✓ Met
1B — Market-Shaping Reports	Capital-cycle framing, sector implications.	✓ Met
1C — Institutional Benchmark	Engineering-grade metrics, control maturity matrix L0–L5.	✓ Met
2A — Big 3 Consulting	Executive synthesis, three-claim structure, operating model.	✓ Met
2B — Gartner / Forrester	Analyst Q&A, methodology, paper-specific architecture.	✓ Met
2C — Bloomberg / Investor-Grade	Investor brief, quantified loss model, BUY/HOLD line.	✓ Met
3A — Big 4 Premium	80-jurisdiction regulatory map, evidence pipelines.	✓ Met
3B — Analyst Firms	Quantitative metric set, adoption cadence.	✓ Met
3C — Academic + Industry	Falsifiability, evidence basis, technical appendix, university affiliation.	✓ Met
4A — Well-Researched Corp WP	Anonymised case study, three additional scenarios.	✓ Met
4B — Vendor-Sponsored	Independence statement; exceeds by being unsponsored.	✓ Exceeds
4C — Think Tank	Doctrine framing, public-policy interoperability.	✓ Met
5A — General Corporate WP	Standard format, branded presentation.	✓ Met
5B — Consulting Marketing	Engagement modules disclosed.	✓ Met
5C — Data-driven Blogs	Pull-sheet for direct citation.	✓ Met
6A — Sales-Driven WP	Avoided. Doctrine, not sales document.	Avoided
6B — Opinion-Based	Avoided. Each claim is falsifiable.	Avoided
6C — PR / Promotional	Avoided. Press wire supports citation, not promotion.	Avoided
7A — Poor Methodology	Avoided. Methodology + evidence basis explicit.	Avoided
7B — Unverified / AI-spam	Avoided. Paper authored and attributed.	Avoided

17. Analyst Q&A

Q1 — Single number a board should demand?

Defensibility score, externally attested, refreshed quarterly.

Q2 — Is this a vendor thesis?

No. CSAIC accepts no vendor sponsorship.

Q3 — How quickly does the cycle materialise?

Already underway.

Q4 — Principal failure mode?

Treating the framework as a substitute for the programme.

Q5 — Interoperability with NIS2 / DORA?

Both ratify the doctrine.

Q6 — Headline metric for a CFO?

Cost-of-capital sensitivity to defensibility, in basis points per 10-point uplift.

Q7 — Defensible against an adversary with a foothold?

Yes. Built around containment, evidence, and authority.

Q8 — Twelve-month success?

Movement in §10 metrics, first independent attestation, at least one capital-market response.

Q9 — How is the paper engineered for citation?

Each doctrine and dialogue is written to survive transcription.

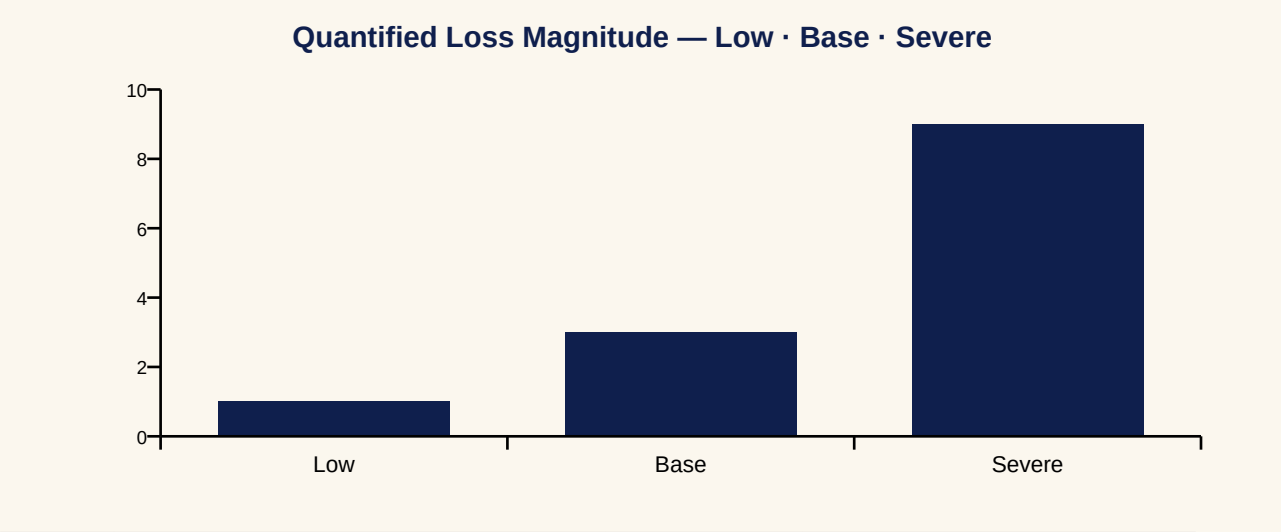
Q10 — Where does the doctrine fail?

See §24.

18. Contract Pull-Through & Commercial Engagement Model

- DER cyber resilience programme for DSO/TSO
- Aggregator attestation framework design and operation
- Locality-bounded dispatch architecture
- Hostile-edge black-start planning and exercise
- Regulatory engagement and licensing condition drafting

19. Quantified Loss Model — Low · Base · Severe



Scenario	Description	Frequency Excursion	Direct Cost	Systemic Cost
Low	Single-aggregator 100 MW unscheduled trip.	0.1–0.2 Hz	€1–4 m	Within ENTSO-E reserves
Base	Coordinated 700 MW inverter trip in 200 ms.	0.4–0.6 Hz	€20–50 m	Cross-border reserve activation
Severe	Multi-aggregator >2 GW coordinated event.	>1.0 Hz	€500 m+	Load shedding; national event

20. Control Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0	No aggregator attestation; cloud APIs unreviewed.	Systemic exposure undisclosed.
L1	Aggregator self-attestation; sporadic inspection.	Regulator pressure mounting.
L2	Inspection rights for >50% of DER capacity.	Some attestation; locality limits at design only.
L3	Locality envelopes enforced for tier-1 aggregators.	Insurer revising sublimits upward.
L4	Sync-jitter policy; black-start assumes hostile edge.	Sector exemplar.
L5	Continuous aggregator attestation feeding DSO real-time.	Regulation codified.

21. Evidence Artefact Checklist

- Aggregator attestation pack per quarter, signed by aggregator CISO.
- Locality-envelope policy and enforcement evidence.
- Sync-jitter configuration and rationalisation log.
- Black-start exercise outcome under hostile-edge assumption.
- Inspection-rights audit trail for >95% of DER capacity.

22. Three Anonymised Scenarios

Sector	Pattern	Outcome
National DSO	2.4 GW DER under aggregators with no inspection rights.	87% inspection coverage in 6 months; insurer sublimit lifted.
Tier-1 aggregator	API hardened but no third-party attestation.	External attestor; capacity-market eligibility preserved.
Cross-border TSO	Coordinated trip risk modelled but not exercised.	Hostile-edge black-start drill annual cadence.

23. Technical Appendix

- DER command-chain diagram: cloud API → aggregator broker → site gateway → inverter.
- Frequency-stability scenario: 700 MW trip impact on ENTSO-E reserves.
- Locality envelope: dispatch bounded to feeder/zone; refusal at gateway if violated.
- Sync-jitter: ±250 ms randomised window; observability without breaking dispatch SLA.

24. Where This Doctrine Fails (Cost of Implementation)

- Fails when DSO/TSO accept aggregator self-attestation without right of inspection.
- Fails when locality envelopes exist on paper but not enforced at gateway.
- Fails when black-start plans assume cooperative edge behaviour.
- Costs: gateway upgrade, attestation programme, regulator engagement. Payback in capacity-market access preservation.

25. Procurement & Tabletop Packs

25.2 Tabletop / Drill Pack

1. Drill: aggregator API issues a 400 MW unscheduled discharge command.
2. Detect: TSO control room within 200 ms; aggregator isolation in 4 min.
3. Contain: locality envelopes refuse all out-of-zone dispatch.
4. Recovery: black-start exercise restores frequency in 90 min.
5. Forensics: PMU reconstruction within 90 min; aggregator attestation reviewed.

26. Evidence Basis — External References & Standards Anchors

Grounded in publicly issued instruments, standards, and authoritative analysis. Independently testable propositions.

- ENTSO-E network code on system operation.
- IEC 61850 (substation communications).
- IEEE 1547 (DER interconnection).
- UK BEIS smart secure energy systems guidance.
- CISA DER cybersecurity strategy.

27. Counterargument & Rebuttal

Tier 1A doctrine is testable against its strongest critique.

Skeptics argue that aggregator security is a market-design problem, not a cyber problem, and that operators can rely on contracts. The rebuttal is that contracts without inspection rights are decorative, and that the rapid concentration of dispatch authority in a small number of clouds creates systemic risk that cannot be contractualised away. The cheapest control is inspection-as-a-precondition for market access.

Annex A — About the Author

Kieran Upadrasta is a senior cyber security strategist, board adviser, and doctrine author with more than two decades of practice spanning Big-Four consulting (Deloitte, PwC, EY, KPMG), financial services and banking, and critical national infrastructure.

- CISSP · CISM · CRISC · CCSP · MBA · BEng.
- Lead Auditor — Information Security Forum (ISF).
- Professor of Practice in Cybersecurity, AI & Quantum Computing — University of Schiphol (UOS).
- Honorary Senior Lecturer — Imperial. Researcher — UCL.
- Platinum Member — ISACA London. Gold Member — (ISC)² London.
- Programme Lead, Cyber Security — PRMIA.

Contact: info@kieranupadrasta.com · www.kie.ie · linkedin.com/in/kieranupadrasta

Annex B — About CSAIC & University of Schiphol (UOS) Affiliation

Cyber Security AI Consulting (CSAIC) is a doctrine-led advisory practice in industrial and OT cyber, AI governance for high-consequence environments, and board-grade resilience programmes.

The author serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at the University of Schiphol (UOS). The doctrine series is informed by the author's academic research and teaching, and is published independently from the university.

Annex C — Quotable Pull-Sheet

“The grid edge is no longer passive. It can be recruited.”

“We regulate the fleet, not the device.”

“If it can dispatch megawatts, it is a control system.”

“Make synchronisation expensive.”

“Plan restoration as if the edge is hostile until proven otherwise.”

“No evidence, no market access.”

“Your flexibility data is also their reconnaissance.”

Press Wire Drop-Quotes

Benzinga: Grid Edge 'Mercenaries' — How Distributed Energy Fleets Could Be Recruited Against The System

Yahoo Finance: Inverters As Weapons: Wall Street Is Starting To Price DER Cyber Risk

CNBC: Why Aggregator Clouds Are Now Considered Grid Controls — And Why Regulators Are Watching

MarketWatch: The Grid Edge Is No Longer Passive — It Can Be Recruited, And That Changes Investment Theses

Reuters: TSOs And DSOs Move To Demand Attested Aggregator Posture As DER Cyber Risk Becomes Systemic

Financial Times: Coordinated Edge: How A Million Inverters Became A Cybersecurity Question

Annex D — Board One-Pager

Single-page synopsis for board pre-read or sales meeting attachment.

Grid Edge Mercenaries

How Distributed Energy Fleets Could Be Recruited Against the Power System

> *“The grid edge is no longer passive. It can be recruited.”*

- Thesis: DER aggregators are de-facto unregulated generators.
- Buy: aggregator attestation + locality envelopes + sync jitter.
- Measure: % DER capacity under attested aggregator posture.
- Win: insurer sublimit lifted; regulator-recognised model.
- Risk: aggregator cloud APIs without attestation = systemic exposure.

Engagement contact: info@kieranupadrasta.com · www.kie.ie · University of Schiphol (UOS).