TELBORG

Data Center Briefing

April 03, 2026

Global

Key themes:
Iranian drones hit AWS ME-SOUTH-1 Bahrain; service impacts; Microsoft commits $5.5bn to Singapore cloud and AI (2025–2029); DayOne plans MYR28bn Malaysia expansion; Johor training for 1,000 engineers; UK grid connection reforms could create two-tier data centre market

Amazon just got a stark reminder that “location risk” isn’t a spreadsheet exercise. An Iranian drone attack reportedly hit AWS’s ME-SOUTH-1 data center in Bahrain on April 1, triggering a fire and service impacts — the second such attack in a month. For anyone underwriting Middle East capacity (or relying on it), this moves physical security and geopolitical escalation from background noise to a line item.

The Big Stories

Iranian drone attacks threaten US tech datacenter investments reports Iranian drones struck Amazon’s ME-SOUTH-1 (Bahrain) facility, causing fire and AWS service impacts, amid IRGC threats against at least 18 US tech firms. Beyond the immediate outage risk, the bigger issue is capital at risk across the region — including Amazon’s previously announced $5.3bn Saudi data center due in 2026. If this pattern holds, “regional hub” strategies start to look more like correlated exposure.

Microsoft to invest $5.5 billion in Singapore cloud and AI is a reminder that, even as security risk rises in some geographies, the demand pull for AI infrastructure is still steamrolling ahead in others. Microsoft’s $5.5bn (2025–2029) commitment is framed as cloud + AI infrastructure and operations, plus a security/governance push. The tell here is Singapore’s continued ability to

attract big-ticket spend despite high costs and tight resource constraints — the premium market is staying premium.

DayOne to invest MYR28bn in Malaysia for data centre expansion underlines why Malaysia keeps winning the "next Singapore" overflow trade. DayOne says it will put more than MYR28bn (~$6.9bn) into Malaysia by end-2026, make the country its largest operating base, and train 1,000+ data centre engineers in Johor. The scale and the workforce angle matter: this isn't just land-and-power arbitrage; it's an attempt to lock in operating talent as AI workloads push complexity (and staffing) up.

UK grid reforms could reshape the data centre market lays out the next battleground: connection queues and who gets to cut the line. DC Byte warns the UK consultation on accelerating network connections for "strategic demand" could effectively create a two-tier market — established operators and priority projects on one side, everyone else pushed toward self-generation or non-firm connections. Translation: incumbency becomes a utility advantage, and speculative land banking looks a lot less clever.

Community pushes back on Valley Link transmission line proposal shows the US version of the same story, just messier. Valley Link (Dominion Energy/Transource/FirstEnergy) is proposing a 115-mile 765kV line in Virginia — ~$1bn, aimed at serving data centers, and "largely expected to be borne by Virginia ratepayers." Strong local opposition is already organized, with more meetings slated before a filing with the Virginia State Corporation Commission. For developers, this is the uncomfortable math: the grid upgrades you need are exactly the ones the public is least willing to host or fund.

Behind the Headlines

India's data centres strain energy, water and urban heat systems puts hard numbers on what "AI scale" does to national infrastructure. CSI estimates India data-centre electricity use rising from ~13 TWh (2024) to ~57 TWh by 2030, and water use from ~150 billion litres (2025) to ~359 billion litres (2030). The policy asks — mandatory PUE reporting, binding renewables and water rules, smarter siting — read like the early innings of a regulatory clampdown. The interesting twist is the linkage to India's Nuclear Energy Mission (INR 20,000 crore in the 2025–26 budget) targeting at least five SMRs by 2033: the

industry is already casting “firm clean power” as the only politically durable answer to growth.

NCC Group warns DC power regulation is a cyber risk is a useful wake-up call for anyone treating electrical infrastructure as “just” engineering. NCC’s point is straightforward: once power regulation becomes digitally controlled — firmware, network interfaces, remote management — it becomes part of the cyber-physical attack surface. Defence-in-depth (secure firmware, trusted boot, network isolation, supplier verification, continuous monitoring) is not optional if you’re running high-density sites where power events can cascade fast. The investor takeaway: resilience capex is shifting from generators and switchgear alone to control-plane security — and that will show up in both build cost and operating discipline.

QuiX demonstrates below-threshold error mitigation in photonic quantum computers is early-stage, but it hints at a future where “data-center integration” includes quantum hardware that doesn’t behave like today’s lab toys. QuiX claims a first net-positive error mitigation result on a photonic processor (including a 2.2× reduction in photon indistinguishability error) and argues that combining this with error correction could cut photon sources per logical qubit by up to 4×. If that direction holds, it’s not just a science milestone — it’s an infrastructure story about shrinking the overhead that keeps quantum confined to bespoke environments. Not imminent revenue for colo, but a signal that the boundary between HPC, AI, and emerging compute keeps getting fuzzier.