YAVA MONTHLY REPORT

DATE: 30.01.2026

ISSUE NO. 15

INSIDE THIS ISSUE

PG. 2-3
World Economic Forum Insights and Cyber Mitigation Strategies

PG. 4-7
Energy resilience, infrastructure security trends, regional deployments & dual-use tech focus

PG. 8
Market outlook for infrastructure resilience and upcoming partnership opportunities



YAVA Monthly Report

Welcome to YAVA's Monthly Report, offering a clear snapshot of our latest projects, regional developments, and sector movements. Each edition includes YAVA project updates, market analysis, and key news from Africa, the Middle East, India, and Europe — delivering practical insight across our operating landscape.

Visit www.yava.com for more.
Or follow us on LinkedIn (@YAVA_COM)



'Contrasting political approaches at Davos highlight a shared shift toward economic sovereignty and infrastructure resilience as instruments of national power.'

Emerging Threats

- **AI Arms Race:** AI is anticipated to be the most significant driver of cybersecurity changes in 2026 by 94% of leaders. While AI can automate complex defence tasks, 87% of organisations identified AI-related vulnerabilities as their fastest-growing risk in 2025.
- **Cyber-Enabled Fraud:** In a major shift, cyber-enabled fraud has overtaken ransomware as the top concern for CEOs. Over 73% of survey respondents were personally affected or knew someone affected by such fraud in 2025.
- **Critical Physical Assets:** Attacks are increasingly targeting critical physical assets, with recent incidents affecting aviation and satellite systems highlighting these vulnerabilities.

WORLD ECONOMIC FORUM 2026: TRUMP VS CARNEY.

Critical infrastructure remains undervalued as a global risk

The World Economic Forum in Davos underscored a growing truth: critical infrastructure has become a central battleground in global economic and political strategy. According to a 2024 Knowbe4 report, cyberattacks on critical infrastructure surged by over 30% globally between 2022 and 2023. These attacks are increasingly causing real-world harm; a Claroty study found that in industries like healthcare, 47% of incidents affected physical systems like medical devices and building management systems.

The Forum's Global Cybersecurity Outlook 2026 report, written in collaboration with Accenture, delves deeper into the shifting landscape:

- **Geopolitics as a Top Driver**: Geopolitical volatility is now the primary factor influencing cyber strategy. In 2026, 64% of organisations are explicitly accounting for geopolitically motivated attacks,
- **Confidence Crisis:** Confidence in national preparedness is eroding. Globally, 31% of respondents report low confidence in their national ability to respond to major cyber incidents.
- **Systemic Supply Chain Risk:** Supply chain vulnerabilities are a leading ecosystem risk. In 2025, 54% of large organisations identified this as a major challenge. The WEF warns of "concentration risk," where reliance on a few critical providers (like the 2024 CrowdStrike outage) can cause cascading losses across entire economies.

This reality was reflected in sharply contrasting political narratives. Canadian Prime Minister Mark Carney, in one of the most widely cited speeches of the forum, argued that volatility, fragmentation, and financial stress are no longer cyclical shocks but structural features of the global system, requiring stronger institutions, coordinated resilience, and long-term investment discipline. His remarks framed infrastructure as the stabilising backbone of an increasingly fragile global economy.

Copyright © 2026

Related Topics

- OpenAI warns new AI models pose high cybersecurity risks (Reuters)
- UK launches £210 million cyber action plan after admitting public sector vulnerability (TechRadar)
- Canada advances telecom cybersecurity bill to protect infrastructure (Global News)
- Germany and Israel partner on "cyber dome" defence initiative (Reuters)
- Finland sets up undersea surveilance to guard critical cables (Reuters)
- Global cybersecurity outlook higlights AI security gap as top concern (World Economic Forum)



Top considerations for cyber risk mitigation strategies

WEF Global Cybersecurity Outlook report

What this means in practice - and where YAVA fits

YAVA was in attendance in Davos, and away from the main stages the same message surfaced repeatedly in closed sessions and operator discussions: infrastructure risk is no longer theoretical, and resilience cannot be improvised once pressure arrives.

As Mark Carney put it in his address,

"resilience is not built in the moment of crisis; it is accumulated quietly over time through sustained investment, coordination, and trust in institutions."

That observation matters because it runs counter to how infrastructure is still too often treated. Too many programmes are triggered reactively, assembled quickly, and justified politically - rather than designed patiently as long-term capability.

In practice, this is where most resilience strategies fail. Cyber is separated from physical systems. Technology is procured without integration into operations. Modernisation is framed as an upgrade rather than an operating posture. When stress arrives, systems exist - but they do not work together.

YAVA's role sits precisely at this fault line. Our work focuses on turning strategic intent into infrastructure that can actually operate under pressure: ports that continue to move cargo, energy systems that absorb volatility, transport and aviation platforms that remain functional during disruption, and digital layers that support decision-making rather than complicate it.

The Davos contrast between Trump and Carney made for sharp headlines, but beneath the politics the direction of travel is shared. Infrastructure is now economic security made tangible. It is national power expressed through continuity.

Those who invest early accumulate resilience quietly, as Carney described. Those who delay discover, often publicly, that fragility itself has become a strategic vulnerability.



USA House at the World Economic Forum in Davos —

Copyright © 2026



Sumit Dubey, Partner and Asia Specialist at YAVA, attended India Energy Week to discuss the secure and accessible future of energy

India Energy Week Exhibition & Conference | 27–30 January. Goa, India

INDIA ENERGY WEEK

Connecting Indian energy ambition with global execution

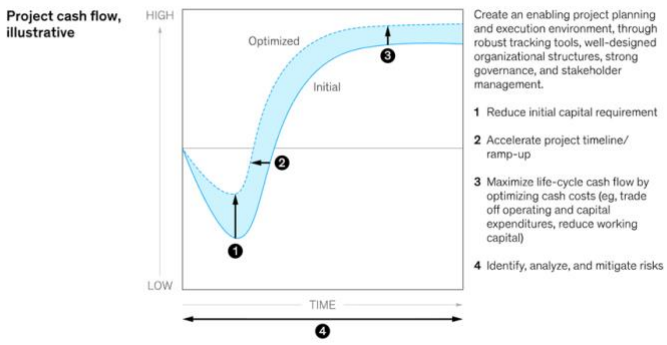
India Energy Week brought together senior leadership from India's energy ecosystem and global stakeholders at a time when energy infrastructure is under mounting geopolitical and financial pressure. While global energy infrastructure investment continues to grow, project risk, security, and execution capacity remain persistent barriers to overseas expansion.

YAVA held detailed conversations with representatives from IOCL, BPCL, ONGC, Petronet, and others. Discussions centred on enabling structured market access, forming durable partnerships, and solving operational delivery in high-need regions such as the Middle East and East Africa. The message was consistent: capital and policy support are increasingly available, but delivery failure, due to poor integration, vendor misalignment, and insufficient local execution, remains a limiting factor.

Data from McKinsey shows that 79% of large infrastructure projects exceed their budgets, and over half fail to meet their scheduled timelines. Embedding operational teams and improving planning can reduce time to delivery, and boost resilience during implementation; approaches that align closely with YAVA's field model and cross-border deployment experience.

- **Volutpat mos at neque nulla lobortis dig nissim convention.**
  Enim neo velit adsum odio, multo, in commoveo quibus premo tamen erat huic.
  Occuro luxor dolore, ut at praemitto opto si sudo, opes feugiat iriure validu.
- **Feugait in obruo quae ingenium tristique elit vel**

Preconstruction excellence addresses all drivers of net present value across the project life cycle.



Source: https://www.mckinsey.com/capabilities/operations/our-insights/seize-the-decade-maximizing-value-through-pre-construction-excellence

- **Volutpat mos at neque nulla lobortis dig nissim convention.**
  Enim neo velit adsum odio, multo, in commoveo quibus premo tamen erat huic.
  Occuro luxor dolore, ut at praemitto opto si sudo, opes feugiat iriure validu.
- **Feugait in obruo quae ingenium tristique elit vel**

Related Topics

- EU fast-tracks cross-border power grid projects to ease energy prices (Reuters)
- Ofgem highlights energy infrastructure resilience as market condition report released (Ofgem)
- Europe's grids face major investment push to meet future demand trends (Energy Infrastructure Partners)
- UK's Planning and Infrastructure Bill becomes law, speeding energy deployment decisions (DLA Piper)
- Six energy tech leaders outperform in early 2026 stock markets (Reuters)
- Mozambique, TotalEnergies relaunch $20 billion LNG project (Reuters)

Copyright © 2026



Italy is bracing for AI-driven threats during the Winter Olympics

INFRASTRUCTURE SECURITY TRENDS TO WATCH

Escalating hybrid threats push resilience to the forefront

- **National cyber defences ramp up for major events:** Italy's cybersecurity teams are intensifying monitoring ahead of the 2026 Winter Olympics, using AI-enabled analysis of dark web activity in response to mounting risks. (Reuters)
- **State-level threats to physical infrastructure persist:** Finnish defence analysts warn that sabotage risks to undersea power, telecom, and pipeline systems in the Baltic Sea remain acute. Disruption to narrow maritime shipping passages or 'chokepoints' affects $192 billion worth of maritime trade every year. (Environmental Change Institute)
- **Critical infrastructure markets expand:** The global data center sector is estimated to grow at a 14% CAGR over the next five years, which could result in 100 GW of new capacity coming online including hyperscale, colocation and on-prem facilities. This equates to $1.2 trillion in real estate asset value creation and a need for roughly $870 billion of new debt financing. This growth is driven by cloud demand and advanced security requirements, reinforcing resilience as both a security and economic priority. (JLL)

Market Growth Projections

The market is experiencing robust growth, with various segments showing strong compound annual growth rates (CAGR):

Metric	2024 Market Size (USD)	2030 Projected Size (USD)	CAGR (Forecast Period)
Overall Market	~$320–$506 billion	~$627–$1,105 billion	~10–19%
Construction	$240.97 billion	$456.50 billion	11.8% (2025-2030)
Support Infrastructure	$57.95 billion	$92.23 billion	8.2% (2025-2030)

Source: https://www.sphericalinsights.com/reports/data-center-market

TECHNOLOGY HIGHLIGHT: DUAL-USE INNOVATION

Defence-grade capabilities accelerating into civilian infrastructure

Dual-use technologies, systems that serve both civilian infrastructure and defence, are moving from policy to deployment. New regulatory frameworks and funding from Europe and beyond are channelling investment into AI, autonomous systems, sensing, and communications tools that meet both operational and security needs.

This matters for civilian operators because defence-grade systems are reaching real-world deployments faster than ever. YAVA plays a key role in translating advanced capability into secure, scalable infrastructure across high-consequence environments.

Copyright © 2026



SPOTLIGHT: TELECOM & CRITICAL NETWORK EQUIPMENT

Sovereignty, security, and the future of connectivity

Telecom infrastructure is increasingly treated as a national strategic asset. In January 2026, EU policymakers advanced proposals to phase out "high-risk" equipment from 5G and fixed-line networks, reflecting deeper concerns about supply chain vulnerability, cyber interference, and sovereignty.

For operators and tech partners, the implications are clear:

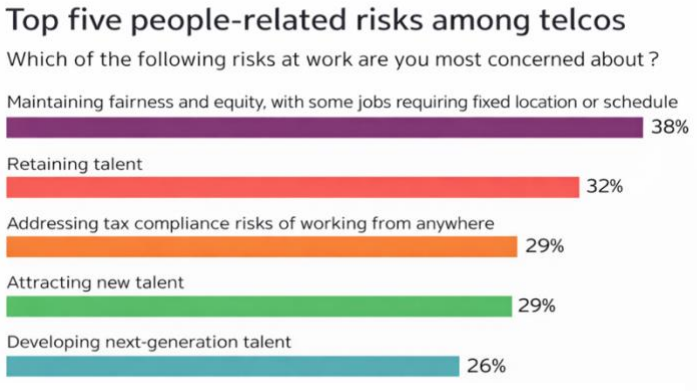
- Supply chain resilience is now a national security issue
- Vendor diversity and system interoperability are strategic advantages
- Network security must extend from core to edge and IoT infrastructure

Telecom infrastructure is now a frontline concern for national security, with policymakers and operators reassessing networks, suppliers, and deployment models in response to rising geopolitical risk

But technical risks are only half the story.

According to *EY's* Top 10 Risks for Telecommunications 2024 report, internal delivery challenges, including poor execution, fragmented governance, and inadequate workforce models, now rank among the most pressing threats facing telecom operators. Integration complexity and change fatigue are eroding performance, even when capital and policy alignment are in place.

YAVA directly addresses this gap by embedding cross-border operational teams work alongside technology deployment from day one, reducing delivery friction, closing execution gaps, and accelerating stabilisation. This model is designed for resilience: built to navigate both geopolitical uncertainty and real-world complexity in high-consequence infrastructure environments.



Source: https://www.ey.com/en_uk/insights/telecommunications/top-10-risks-for-telecommunications

Copyright © 2026

Related Topics

- AfDB seeks Arab partners to bridge Africa's Infrastructure Finance Gap (Reuters)
- Everstream Analytics 2026 Supply Chain Risk report (Supply Chain Brain)
- Libya signs $2.7 billion partnership to expand Misurata Free Zone (Reuters)
- Marsh 2026 Supply Chain Trends Research (Marsh)
- UNCTAD Review of Maritime Transport 2025 (United Nations)
- Vietnam targets $5.5 billion in foreign loans to boost infrastructure (Reuters)
- India's Adani to bid for 11 airports in $11 billion expansion plan (Reuters)
- Pax Silica Initiative (US Department of State)



Resilience at scale: Reinforcing critical trade infrastructure

In high growth but high-risk markets, infrastructure is expanding rapidly alongside rising pressure from security, climate, and logistics disruption. Under the 'Baku to Belém Roadmap,' the global community has set a target to mobilise $1.3 trillion annually by 2035 for emerging-market resilience, with development banks increasingly mandating cyber and operational security criteria as a condition for this finance.

GLOBAL DEPLOYMENT IN ACTION

The European Bank for Reconstruction and Development (EBRD) includes digital technology development and enhanced cybersecurity as core enablers for achieving broader economic resilience in its 2026-2030 Strategic and Capital Framework.

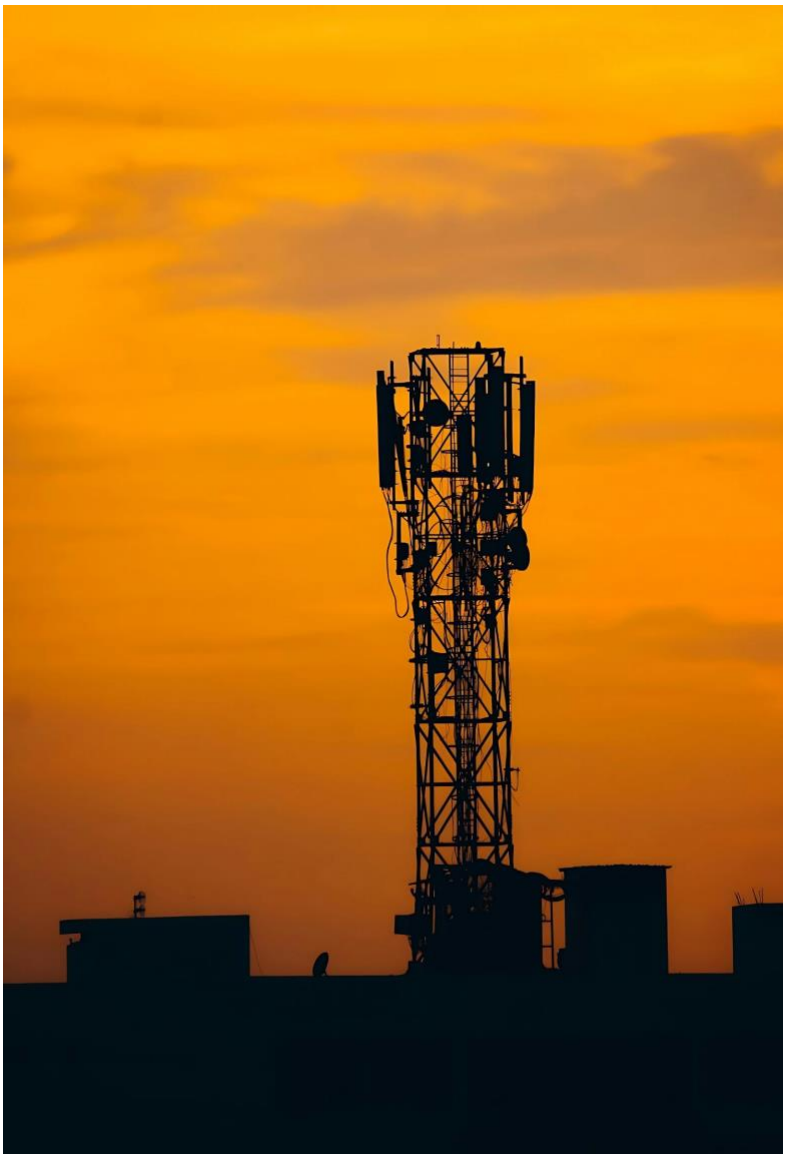
YAVA's deployments reflect these realities, including:

- Keeping airports operational during shocks
- Enhancing logistics visibility and route planning
- Supporting energy operators with limited on-ground capacity
- Partnering on resilience assessments ahead of regional summits





Copyright © 2026



Co-developing the future of infrastructure security – from ports to code

The financial impact is clear: a Tier-1 port outage could disrupt over $100bn in trade, and cyber-induced plant shutdowns like the 2025 Jaguar Land Rover case have triggered losses exceeding $1.9bn across the supply chain.

YAVA is expanding its presence in secure communications, dual-use systems, and autonomous capability to meet these challenges. In this climate, cross-sector partnerships will determine how effectively infrastructure can adapt to structural risk. YAVA remains focused on building those alliances to deliver resilient infrastructure at scale.

YAVA's Event Calender

- India AI Impact Summit, February 16-20
- teissLondon2026 | The European Information Security Summit, February 26
- Cloud & AI Infrastructure London, March 4-5
- Critical Infrastructure Protection & Resilience North America, March 10-12
- Black Hat Asia, Singapore, April 21-24
- RSA Conference 2026, May 4-7

LOOKING AHEAD: PARTNERSHIPS & GROWTH OPPORTUNITIES

Sovereignty, security, and the future of connectivity

As 2026 unfolds, infrastructure security is being shaped by accelerating technology shifts and rising geopolitical fragmentation. AI is driving investment in intelligent monitoring, threat detection, and automated response. Meanwhile, sovereignty and regulatory enforcement, through tools like Europe's NIS2, are raising the bar for accountability and operational readiness.

Insurance markets are reacting accordingly. War-risk premiums for ships in the Middle East surged by over 60% in 2025, while cyber-related insurance costs for infrastructure operators in conflict zones have climbed due to escalating attacks.

For enquiries relating to the topics, commentary, or content in this report, please contact **Nick Ismail** at **nick.ismail@yava.com**, or reach out to our media team at help@yava.com.

When emailing the media team, please use the subject line **"Media Team – Issue (Report Number)"** to help us respond efficiently.

Copyright © 2026

Disclaimer and Confidentiality Notice

This monthly report (the "Report") is issued by YAVA London Ltd ("YAVA") on a confidential basis and is provided solely for informational and discussion purposes. It is intended exclusively for the designated recipient(s) and may not be copied, reproduced, redistributed, forwarded, quoted, or otherwise disclosed, in whole or in part, to any third party without YAVA's prior written consent.

The Report contains a curated summary of YAVA's activities, observations, and perspectives, including but not limited to: operational updates, regional and sector commentary, infrastructure and security themes, geopolitical context, execution insights, and internally derived assessments. Certain references may relate to governments, public authorities, private organisations, supranational bodies, or security-sensitive environments. Portions of the content may therefore be commercially sensitive, politically sensitive, operationally sensitive, or subject to confidentiality obligations.

By accessing, receiving, or reviewing this Report, the recipient acknowledges and agrees to the following conditions:

Confidentiality and Restricted Use

All information contained herein is confidential and proprietary to YAVA. The Report is provided for the recipient's internal use only and must not be used for external briefing, publication, marketing, solicitation, or secondary analysis without YAVA's express written approval.

Non-Circumvention and Relationship Protection

Recipients agree not to directly or indirectly contact, solicit, engage, or seek to establish independent relationships with any clients, counterparties, partners, stakeholders, or entities referenced in the Report. Any attempt to circumvent YAVA's role in current or prospective engagements may constitute a material breach and may give rise to legal or equitable remedies.

No Offer, No Advice, No Reliance

This Report does not constitute, and should not be construed as, an offer, solicitation, recommendation, or endorsement of any service, engagement, transaction, or course of action. It does not provide legal, regulatory, operational, or professional advice. Nothing in this Report creates or implies any advisory, fiduciary, contractual, or agency relationship between YAVA and the recipient.

Observational Commentary and Forward-Looking Content

The views, commentary, and thematic analysis expressed reflect YAVA's observations and internal perspectives as of the date of publication. Certain statements may be forward-looking or indicative in nature and are inherently subject to uncertainty, evolving conditions, and factors outside YAVA's control. Actual outcomes may differ materially from any expressed or implied views.

Sources and Accuracy

Information contained in this Report may be derived from a combination of publicly available sources, partner discussions, governmental communications, industry dialogue, and YAVA's internal activities. While such sources are believed to be reliable, YAVA does not represent or warrant the accuracy, completeness, or continued relevance of the information, and undertakes no obligation to update or revise the content.

Limitation of Liability

To the fullest extent permitted by law, YAVA, its directors, officers, employees, consultants, and affiliates shall not be liable for any loss, damage, cost, or expense, whether direct, indirect, incidental, or consequential, arising from the use of, reliance upon, or interpretation of this Report or its contents.

Governing Law and Jurisdiction

This Report and any matters arising from or relating to its use shall be governed by the laws of England and Wales. The courts of London, United Kingdom, shall have exclusive jurisdiction.

Copyright © 2026