YAVA MONTHLY REPORT

DATE: 27.02.2026

ISSUE NO. 16

INSIDE THIS ISSUE

PG. 2-3
India AI Impact Summit

PG. 4-6
Satellites and connectivity, infrastructure security trends, regional deployments & dual-use tech focus

PG. 7
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)



The world's largest ever AI conference, attended by world leaders and CEOs, took place in New Dehli this February.

Image source: Ludovic Martin, Getty Images

AI Developments

- **AI Infrastructure Acceleration:** Global AI-related capital expenditure continues to rise, with hyperscale cloud providers increasing infrastructure budgets by double digits year-on-year to meet model training and inference demand.
- **AI Security Exposure:** A growing proportion of organisations report AI-enabled cyber threats as a top-tier operational risk, particularly in sectors integrating AI into logistics, energy management, and telecom networks.
- **Regulatory Tightening:** Governments across Europe, India, and North America advanced AI governance frameworks in February, signalling a shift from innovation-first policies toward resilience-first implementation standards.

INDIA AI IMPACT SUMMIT 2026

AI infrastructure becomes a strategic national asset

The India AI Impact Summit underscored a structural shift: artificial intelligence is no longer treated purely as a technology sector opportunity — it is being positioned as sovereign infrastructure. Discussions across policy leaders, cloud providers, semiconductor firms, and defence stakeholders reflected a clear theme: compute capacity, data governance, and AI model development are now instruments of economic security.

India's national AI strategy aligns with broader global trends. According to McKinsey, AI could contribute up to $23 trillion to global GDP by 2040, with emerging markets representing a disproportionate share of growth potential. However, while 88% of organisations now use AI in at least one function, only one-third have successfully scaled it across the entire enterprise. This suggests that while the *potential* GDP figure has grown, the "value at scale" remains a hurdle for many companies.

At the same time, infrastructure demands are accelerating rapidly. The International Energy Agency estimates that global data centre electricity consumption will double from its 2024 to reach 945 TWh by 2030, driven largely by AI workloads. India's own digital economy is projected to reach $1 trillion by 2030, creating mounting pressure on secure compute infrastructure, resilient connectivity, and energy reliability.

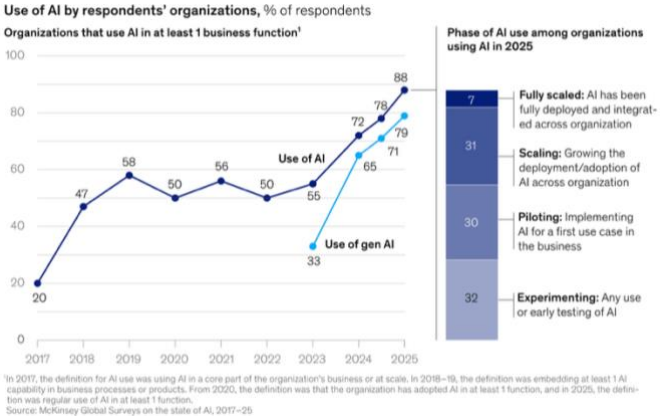
The Summit reflected three structural dynamics shaping AI deployment:

- **Sovereign Compute as National Strategy:** Governments are increasingly investing in domestic AI compute capacity to reduce reliance on external providers. Gartner forecasts that by 2027, 35% of nations will be locked into region-specific AI platforms
- **AI Infrastructure Investment Surge:** Global spending on AI infrastructure is projected BY IDC to exceed $758 billion annually by 2029, with hyperscale data centres, semiconductor manufacturing, and advanced cooling systems driving capital allocation (
- **Security and Critical Infrastructure Convergence:** The World Economic Forum's latest outlook highlights that AI-related cyber risks are among the fastest-growing threat vectors, while Deloitte notes that over over 75% of companies in key sectors, including critical infrastructure, are now investing in Agentic AI to automate complex end-to-end operational processes, increasing both efficiency and attack surface exposure.

Copyright © 2026

Related Topics

- Cybersecurity elevated as national priority as AI expands threat landscape (The Economic Times of India)
- JPMorgan expands $1.5T security & resiliency initiative including AI, critical infrastructure (Reuters)
- Bharti Airtel and Zscaler launch AI & Cyber Threat Research Center in India (Intelligent CISO)
- India AI Impact Summit draws global support and infrastructure commitments (Fortune)
- AI Summit in India promotes a "third way" between U.S. and China in AI governance (Le Monde)



Reported use of AI in at least one business function

McKinsey State of AI report, 2025

What this means in practice - and where YAVA fits

YAVA was present during discussions surrounding AI infrastructure strategy this month, and away from the main stages a consistent message emerged in operator briefings and institutional sessions: AI capability without infrastructure resilience introduces systemic risk.

Compute can be procured rapidly. Models can be deployed at scale. But operational continuity cannot be improvised once pressure arrives.

AI infrastructure depends on three foundational layers — power reliability, secure connectivity, and governed integration into physical systems. When those layers are fragmented, vulnerability compounds. Data centres require resilient energy supply. AI-driven logistics systems depend on uninterrupted telecom networks. Smart grid optimisation tools rely on secure cross-border digital flows. When stress events occur, systems exist — but they do not operate cohesively.

Too often, AI deployment is framed as a digital upgrade rather than an operational transformation. Cyber is separated from physical systems. Connectivity is treated as bandwidth rather than resilience architecture. Governance frameworks lag behind deployment velocity.

This is precisely the fault line where YAVA operates.

Our work focuses on translating strategic intent into infrastructure that functions under pressure:

- Ports and trade corridors supported by secure hybrid connectivity
- Energy systems reinforced with resilient operational visibility
- Aviation and transport platforms integrated with hardened communications layers
- Multi-region deployments aligned with sovereign regulatory requirements

As AI infrastructure expands across critical sectors, resilience becomes the differentiator. The strategic question is no longer whether AI will be deployed — it is whether it will remain operable during disruption.

The India AI Impact Summit reinforced what is increasingly visible across regions: infrastructure is economic security made tangible. Digital capability without operational durability creates fragility. Those who embed resilience early accumulate strategic advantage quietly. Those who separate technology from infrastructure governance discover the gap publicly.

YAVA's role is to close that gap — integrating connectivity, security, engineering capability, and government advisory into systems designed to endure volatility rather than react to it.

Copyright © 2026



Telecom networks face rising strategic threats from cyber and supply chain risk

INFRASTRUCTURE SECURITY TRENDS TO WATCH

Escalating hybrid threats push resilience to the forefront

- **Telco infrastructure targeted by espionage actors:** Singapore disclosed that a cyber espionage group breached elements of four major telecom operators last year, prompting enhanced cooperation between industry and government to harden network resiliency. (Reuters)

- **Critical energy infrastructure struck in Ukraine:** Russia launched a sustained missile and drone campaign against Ukrainian energy grids this month, damaging regional power nodes and underscoring the vulnerability of electricity systems during conflict. (Reuters)

- **Geopolitical flashpoints amplify infrastructure exposure:** Rising US-Iran tensions in the Gulf and escalating organised crime fragmentation in Mexico highlight how energy corridors, shipping routes, and industrial assets can quickly become operational pressure points, reinforcing the need for resilient communications and monitoring systems. (BBC)

- **Rapidly rising cyberattack volume on critical systems:** Swiss authorities reported more than 260 cyber incidents targeting critical infrastructure since late 2025, illustrating persistent pressure on utilities, telecoms, and public services. (B2B Cybersecurity)

- **AI-powered threats foiled in the Gulf:** UAE cybersecurity authorities successfully repelled a large, sophisticated AI-driven cyberattack aimed at gov. digital infrastructure. (The Times of India)

TECHNOLOGY HIGHLIGHT: DUAL-USE INNOVATION

Defence-grade capabilities accelerating into civilian infrastructure

• **AI & cyber research centres expand:** At the India AI Impact Summit, Bharti Airtel and Zscaler announced a new AI & Cyber Threat Research Centre to accelerate advanced defence capabilities and safeguard critical infrastructure sectors like energy and telecom. (The Times of India)

• **Satellite commercial defence contracts rise:** Commercial EO satellite operator Vantor won a US National Geospatial-Intelligence Agency contract for terrain-change detection — a dual-use capability bridging infrastructure monitoring and national security geospatial workflows. (Vantor)

• **Orbital compute concepts accelerate:** SpaceX filed proposals and planning documents for an expanded "orbital data centre" constellation to support AI compute and enhanced connectivity — a technological frontier where infrastructure and space systems converge. (Tech Startups)

• **Automated cyber attack tactics evolve:** Recent threat reporting shows attackers are embedding AI into phishing and exploit campaigns, generating polymorphic threats at scale and expanding attack surfaces on critical networks. (Integrity 360)

Copyright © 2026



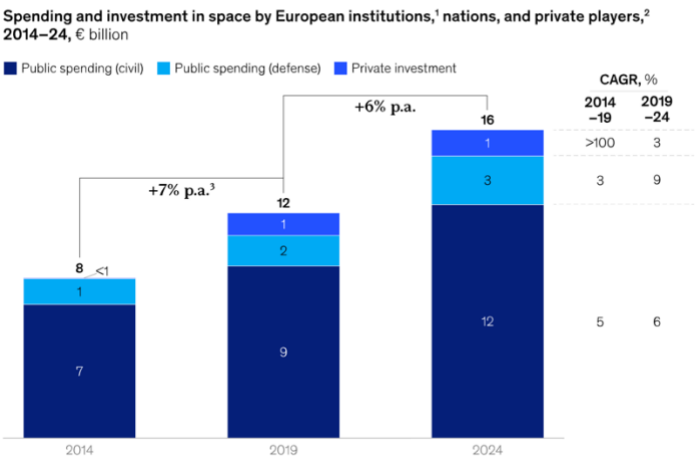
Low Earth Orbit (LEO) satellite constellations are becoming a core layer of national infrastructure resilience, supporting hybrid connectivity across energy, aviation, maritime and remote industrial systems.

SPOTLIGHT: SATELLITES AND HYBRID CONNECTIVITY

Satellite infrastructure is rapidly shifting from niche connectivity solution to strategic national asset. Across Europe, India, the Middle East and North America, governments are accelerating sovereign satellite programmes, expanding Low Earth Orbit (LEO) constellations, and integrating space-based communications into critical infrastructure resilience planning. What was once redundancy is becoming primary architecture.

This reflects deeper concerns around geopolitical fragmentation, subsea cable vulnerability, terrestrial network disruption, and digital sovereignty. According to the UN, 99% of global data traffic travels via subsea cables, leaving national systems exposed to concentrated physical risk. At the same time, the global space economy is projected to exceed $1.8 trillion by 2035 (McKinsey 2025 Space Outlook), with satellite connectivity representing one of the fastest-growing segments.

European space spending and investment have grown steadily and substantially since 2014.



Source: McKinsey

For operators and policymakers, the implications are clear:

- **Resilience through orbit diversification:** LEO, MEO, and GEO architectures provide redundancy against terrestrial outages, natural disasters, and conflict-related disruption. The global satellite broadband market is projected to grow at over 13% CAGR through 2030, driven by government and enterprise demand.

- **Sovereign space capability as strategic leverage:** Europe's IRIS² programme, India's expanding space-based connectivity strategy, and Gulf sovereign investments signal that space infrastructure is now tied directly to economic security and defence posture.

- **LEO spend entering mainstream infrastructure markets:** Gartner forecasts that global spending on low Earth orbit (LEO) satellite communications services will reach $14.8 billion in 2026, up ~25 % year-on-year — with resilience, IoT, maritime/aviation, and enterprise broadband as key growth segments. This reflects LEO's transition from remote connectivity to a core hybrid network layer supporting both commercial and critical infrastructure use cases.

Against this backdrop, recent research highlights the scale of acceleration. According to the first Look Up × Le Point Space Barometer, as of October 1, 2025, there are 13,026 active satellites orbiting Earth; a 23 % year-on-year increase and a more than sixfold rise compared to six years ago. This is largely driven by LEO constellation deployments. Meanwhile, satellite-enabled IoT connections are forecast to exceed 30 million active devices by 2030, expanding use across logistics, utilities, and environmental monitoring.

This shifts the focus from connectivity as reach to connectivity as assured continuity. Satellite networks are no longer supplementary links — they are integral layers within secure national infrastructure systems, supporting trade corridors, offshore energy assets, remote mining operations, aviation routing, and military-civil dual-use communications.

Copyright © 2026

Related Topics

- AI-assisted threat actor compromises 600+ FortiGate devices across 55 countries (The Hacker News)
- US Treasury issues AI use and risk management resources for financial sector (US Department of the Treasury)
- Google Cloud calls for unified AI defense as energy sector faces cyber "perfect storm" (Industrial Cyber)
- Meta and NVIDIA announce long-term infrastructure partnership for AI-optimized data centers (META)
- AI infrastructure sovereignty concept gains traction in academic research (ArXiv)
- EBRD supports critical infrastructure in Turkish cities (European Bank for Reconstruction and Development)

Resilience at scale amid geopolitical uncertainty

In high-growth but high-risk markets, infrastructure expansion is accelerating — but so is exposure. Trade corridors, airports, energy networks, and urban systems are scaling rapidly against a backdrop of geopolitical fragmentation, climate volatility, and digital interdependence. Escalating tensions in the Gulf illustrate how quickly energy infrastructure, shipping lanes, and regional communications networks can become exposed. Similarly, fragmentation of organised crime groups in parts of Latin America has increased pressure on transport routes, mining assets, and industrial operations. Capital is available and policy frameworks are advancing, yet the gap between investment intent and operational delivery remains material.

Across emerging and frontier environments, projects are constrained by limited on-ground capacity, fragmented regulatory ecosystems, and uneven digital maturity. Cyber and physical systems are still too often deployed in parallel rather than as integrated architectures. When stress events occur — whether geopolitical, criminal, climatic, or technological — resilience gaps become visible quickly.

YAVA's work reflects this reality: resilience must be engineered deliberately at system level — across digital, physical, and governance layers.

Our recent deployments and advisory engagements include:

- Maintaining airport and aviation continuity during high-risk events, integrating secure communications and operational visibility into live transport environments
- Enhancing logistics and trade corridor transparency, combining hybrid connectivity with real-time decision-support systems to reduce disruption risk

GLOBAL DEPLOYMENT IN ACTION

- Supporting energy operators in geopolitically exposed regions, deploying secure remote monitoring and hybrid communications where terrestrial infrastructure is fragile
- Advising governments and city authorities on AI-enabled urban resilience, integrating data governance and incentive-driven smart systems to strengthen safety, engagement, and service delivery

In parallel, our smart-city and AI work reinforces a broader principle: resilience is not purely defensive. Operational visibility, coordinated response capability, and intelligent system design improve both stability and performance. In environments affected by geopolitical tension or organised criminal disruption, infrastructure operators require continuous monitoring, secure coordination platforms, and reliable communications to maintain control of assets under pressure.

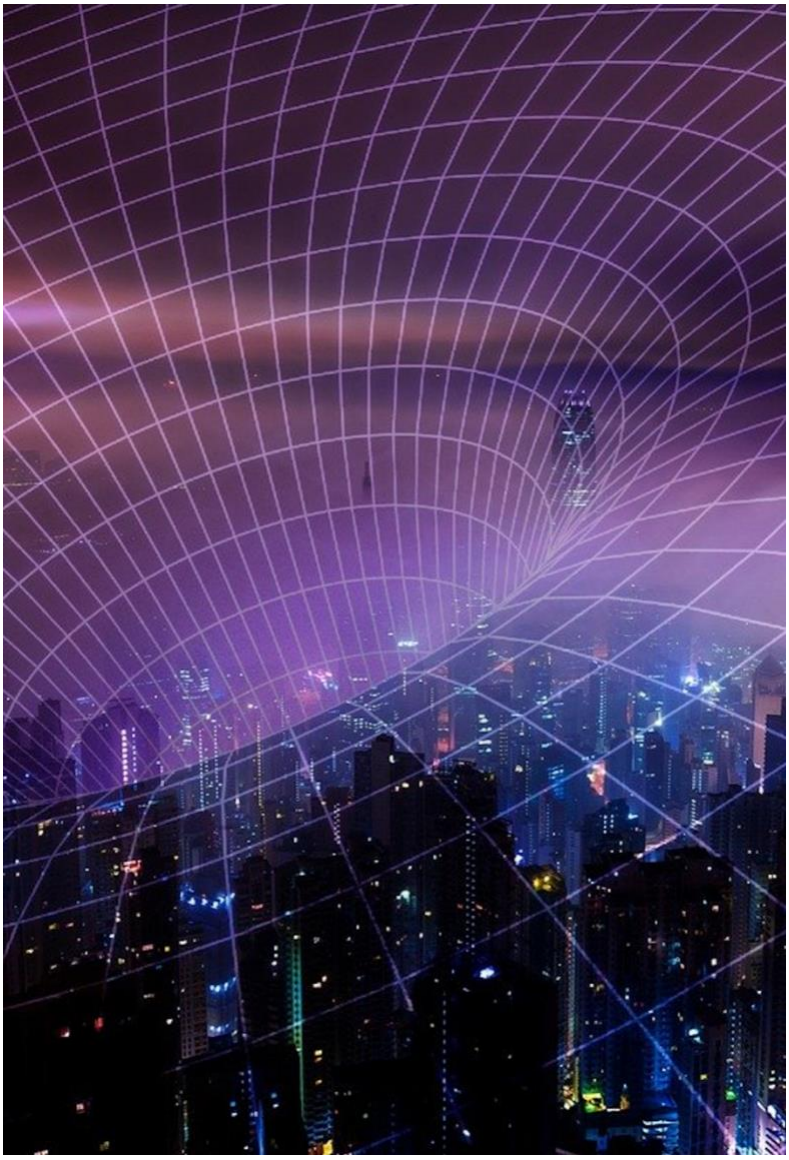
In practice, YAVA operates at the intersection of engineering execution and sovereign alignment. We enable secure decision-making in complex regulatory contexts, coordinate multi-region deployments, and architect systems that function reliably where local capacity is limited.

This integrated approach supports:

• Continuity of trade and energy flows
• Operational stability during geopolitical or security shocks
• Secure adoption of AI and hybrid connectivity
• Transition from reactive response to structured resilience

As infrastructure systems become more digitally integrated and geopolitically exposed, resilience is no longer a technical overlay — it is a strategic capability. The differentiator is not access to capital or technology alone, but the ability to translate strategic ambition into operational durability.

Copyright © 2026



LOOKING AHEAD: PARTNERSHIPS & GROWTH OPPORTUNITIES

Infrastructure resilience in an era of structured volatility

The first months of 2026 have reinforced a central reality: infrastructure is no longer operating in a cyclical risk environment — it is navigating structural volatility. AI acceleration, satellite expansion, energy transition, and geopolitical fragmentation are converging into a more complex operating landscape for governments and critical infrastructure operators.

Capital deployment continues at scale. Global AI infrastructure spending is rising sharply, satellite communications services are growing, and data centre expansion remains in double-digit growth territory. Yet exposure is expanding alongside investment. Digital systems are increasingly intertwined with physical assets, and resilience gaps are no longer confined to the cyber domain — they are operational.

Co-developing the future of resilience, secure communications and hybrid connectivity

In this environment, partnerships become strategic enablers rather than commercial add-ons. No single operator controls the full resilience stack. Satellite providers, terrestrial telecom networks, energy operators, cloud platforms, defence innovators, and regulators are increasingly interdependent.

YAVA's focus remains consistent: integrating secure communications, hybrid connectivity, engineering capability, and government advisory into infrastructure systems designed to operate under pressure. Our work across ports, aviation, energy, and remote industrial environments reflects a simple principle — resilience must be engineered deliberately, not retrofitted reactively.

As infrastructure risk becomes more visible, those who invest early in secure integration, sovereign alignment, and operational continuity will accumulate structural advantage. The opportunity ahead is not merely technological expansion — it is coordinated resilience at scale.

YAVA's Event Calender

- **teissLondon 2026 | The European Information Security Summit**
  London, UK | 26 February | Link
- **Cloud & AI Infrastructure London**
  London, UK | 4–5 March| Link
- **Critical Infrastructure Protection & Resilience North America**
  North America | 10–12 March| Link
- **Black Hat Asia**
  Singapore | 21–24 April| Link
- **RSA Conference 2026**
  San Francisco, USA | 4–7 May| Link

For enquiries relating to the topics, commentary, or content in this report, please contact our media team at media@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