YAVA MONTHLY REPORT

DATE: 31.03.2026

ISSUE NO. 17

INSIDE THIS ISSUE

PG. 2-3
US-Iran tensions and infrastructure resilience

PG. 4
Infrastructure security trends & dual-use innovation

PG. 5
Oil and gas infrastructure spotlight

PG. 6
Global deployment in action: assured access to orbit

PG. 7
Partnerships, resilience, and market outlook



Image source: Khalil Ashawi/Reuters

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)



Rising tensions in the Gulf are exposing critical energy infrastructure and shipping routes to disruption, highlighting the growing importance of resilience in global trade system

Image source: AP

War and Geopolitical Developments

- **Gulf tensions escalate infrastructure risk:** Rising US–Iran tensions in March have increased exposure across the Strait of Hormuz, where energy flows, shipping lanes, and communications systems intersect under geopolitical pressure
- **Energy infrastructure becomes strategic target:** Attacks on oil and gas facilities across the Middle East highlight the vulnerability of upstream and processing assets during regional escalation
- **Hybrid disruption expands beyond physical attacks:** Increased reports of GPS interference and electronic disruption in contested regions signal a shift toward integrated cyber and physical threat environments

US-IRAN ESCALATION

Infrastructure resilience under geopolitical pressure

Escalating tensions between the United States and Iran in March have reinforced a structural reality: critical infrastructure is increasingly exposed to geopolitical confrontation. Maritime security incidents in the Gulf, alongside heightened military posturing, have placed energy corridors, shipping routes, and regional communications networks under renewed pressure.

The Strait of Hormuz remains a central point of vulnerability. Approximately 20% of global oil supply passes through the corridor, making it one of the most strategically sensitive infrastructure chokepoints in the world. Disruption — whether kinetic, cyber, or hybrid — has immediate global consequences for energy markets, logistics systems, and downstream industrial activity.

At the same time, the nature of risk is evolving. Infrastructure exposure is no longer limited to physical disruption. Hybrid threats, including cyber intrusion, GPS interference, and communications disruption, are increasingly integrated into geopolitical strategy. Recent reporting indicates a rise in electronic interference affecting maritime navigation systems in contested regions, highlighting the convergence of digital and physical risk.

Three structural dynamics are becoming increasingly visible:

- **Energy corridors as strategic leverage:** Oil and gas infrastructure is no longer just economic — it is geopolitical. Disruption risk in transit routes now carries systemic implications for global markets.

- **Hybrid threat integration:** Cyber, communications disruption, and physical interference are being deployed in parallel, reducing response time and increasing operational complexity.

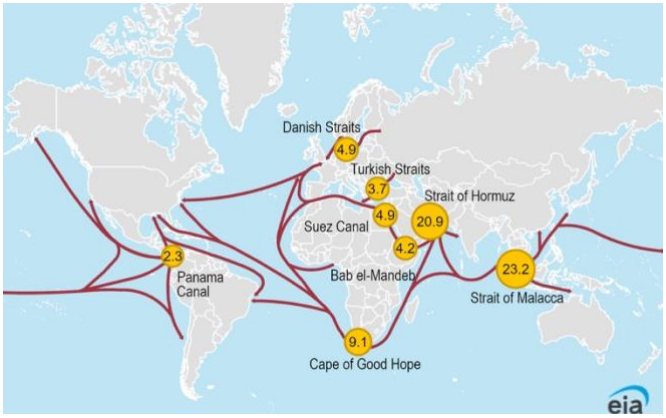
- **Resilience as operational requirement:** Continuity is no longer assumed. Infrastructure must be designed to function through disruption, not recover after it.

This convergence of geopolitical pressure and infrastructure exposure is reshaping how resilience is defined in practice. Energy systems, logistics networks, and communications infrastructure are no longer operating independently. Disruption in one layer can rapidly cascade across others, amplifying both economic and operational impact. As a result, resilience is shifting from redundancy-based planning toward sintegrated systems that maintain visibility, coordination, and control under sustained pressure.

Copyright © 2026

Related Topics

- US disrupts botnets infecting over 3 million devices, highlighting systemic cyber risk (Reuters)
- White House pushes major AI legislation as security risks move into national infrastructure domain (Reuters)
- Oil prices rise as investors assess Middle East escalation and supply disruption risks (Reuters)
- Iran conflict disrupts global LNG supply after damage to key Qatari infrastructure (Wall Street Journal)
- Iran conflict delays major European energy infrastructure projects due to shipping disruption (The Guardian)



Global energy chokepoints highlight systemic infrastructure exposure to disruption

Source: US Energy Information Administration

What this means in practice - and where YAVA fits

Discussions across operators and government stakeholders this month reflected a consistent message: infrastructure exposure in geopolitical environments is no longer theoretical; it is operational.

Systems are being deployed into environments where disruption is expected, not exceptional. Energy infrastructure must operate under contested conditions. Ports and logistics systems must maintain throughput despite security volatility. Communications networks must remain stable even when interference is deliberate.

The challenge is maintaining control of infrastructure.

Infrastructure resilience in this context depends on three operational layers: continuous visibility, secure communications, and coordinated response capability. When these layers are fragmented, disruption compounds quickly. When they are integrated, systems remain operable even under pressure.

Too often, resilience strategies are still treated as contingency planning. Monitoring systems are deployed without integration into decision-making. Communications systems are implemented without redundancy. Cyber and physical infrastructure remain separated.

When stress arrives, systems exist but they do not function together.

This is precisely where YAVA operates.

Our work focuses on enabling infrastructure operators and governments to maintain visibility, coordination, and control in complex environments:

- **Energy and maritime systems supported with resilient communications layers**, ensuring operational continuity across exposed corridors
- **Transport and logistics platforms integrated with real-time monitoring and decision-support systems**, reducing disruption risk in volatile regions
- **Multi-region deployments aligned with sovereign and regulatory requirements**, ensuring infrastructure remains operable across fragmented environments
- **Secure hybrid connectivity architectures**, combining satellite, terrestrial, and mobile networks to maintain communications under stress

As geopolitical pressure increases, the differentiator becomes infrastructure operability.

The strategic question is no longer whether disruption will occur, but whether systems will continue to function when it does.

Copyright © 2026



Gulf energy infrastructure faces disruption as geopolitical tensions escalate

Image source: AFP via Getty Images

INFRASTRUCTURE SECURITY TRENDS TO WATCH

Escalating hybrid threats push resilience to the forefront

- **Maritime and energy infrastructure exposed in the Gulf:** Rising US-Iran tensions in March have increased risk across the Strait of Hormuz, with energy exports, shipping routes, and regional communications networks facing heightened disruption exposure. (Reuters)
- **Iran warns of escalation after attacks on energy infrastructure:** Tehran signalled it would show "zero restraint" following strikes on key gas facilities, highlighting the vulnerability of global LNG supply chains and energy infrastructure. (The Guardian)
- **UK expands cyber cooperation to support infrastructure resilience in Ukraine:** New platform connects international firms with cyber resilience projects, reinforcing coordinated defence of critical infrastructure. (UK Government / DSIT)
- **Subsea infrastructure resilience moves up the agenda:** The UK and Ireland launched joint readiness exercises to prepare for undersea cable disruption, reflecting growing concern over critical digital infrastructure exposure. (LSE)
- **AI lowers barrier for cyberattacks at scale:** New research shows AI tools are enabling more sophisticated phishing, malware generation, and cyber campaigns targeting infrastructure systems. (Infosecurity Magazine / Cloudflare)

TECHNOLOGY HIGHLIGHT: DUAL-USE INNOVATION

Defence-grade capabilities accelerating into civilian infrastructure

• **AI governance moves into national security domain:** The White House advanced plans for a major federal AI framework, reflecting growing concern over AI's role in both cyber defence and infrastructure vulnerability. (Reuters)

• **Satellite communications investment aligns with sovereign defence priorities:** European operators continue to expand investment in next-generation satellite systems, including IRIS², reinforcing the convergence of defence capability and critical infrastructure connectivity. (SpaceNews)

• **Cyber capabilities become automated and scalable:** The disruption of global botnets affecting millions of devices highlights how automated infrastructure is being used in cyber operations, increasing systemic risk across connected systems. (Reuters / CISA)

• **AI-driven threat environments expand across infrastructure sectors:** New threat intelligence shows AI being used for malware generation, reconnaissance, and coordinated attacks, accelerating both capability and complexity in cyber operations. (DNV Cyber / Infosecurity Magazine)

Copyright © 2026

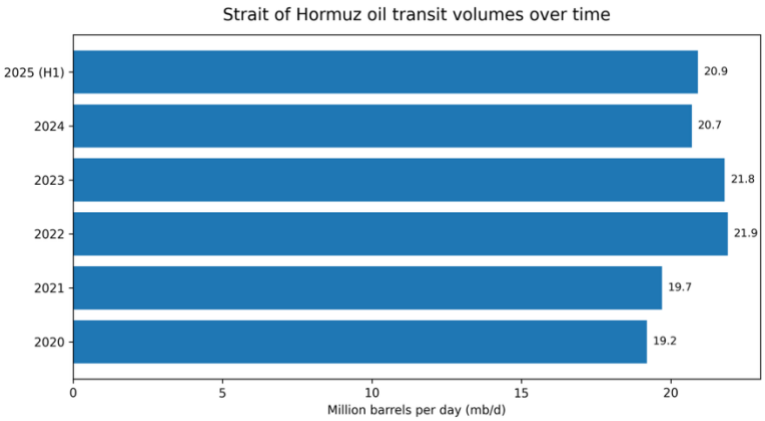


SPOTLIGHT: OIL AND GAS INFRASTRUCTURE

Oil and gas infrastructure is increasingly positioned at the centre of geopolitical and operational risk. March developments in the Gulf reinforced how quickly energy systems can become exposed to disruption, with upstream production, midstream transport, and downstream processing all affected by instability across key regions.

This reflects deeper structural pressures. According to the International Energy Agency, global oil demand is expected to remain above 100 million barrels per day through 2026, maintaining reliance on complex, globally distributed supply chains. At the same time, energy infrastructure is becoming more digitally integrated, increasing exposure to cyber and hybrid threats.

This concentration of demand through a small number of strategic transit routes means that disruption risk is not evenly distributed. Certain corridors carry disproportionate weight within the global energy system, making them critical pressure points during periods of conflict or instability. The Strait of Hormuz is the clearest example: a single chokepoint through which a significant share of global oil flows continues to pass. The chart below illustrates how volumes through Hormuz have remained consistently high in recent years, reinforcing its importance to energy security and infrastructure resilience.



Source: US Energy Information Adminstration

Oil and gas infrastructure is increasingly exposed to geopolitical disruption, with energy corridors, export terminals and shipping routes becoming central to operational resilience and market stability

For operators, the implications are clear:

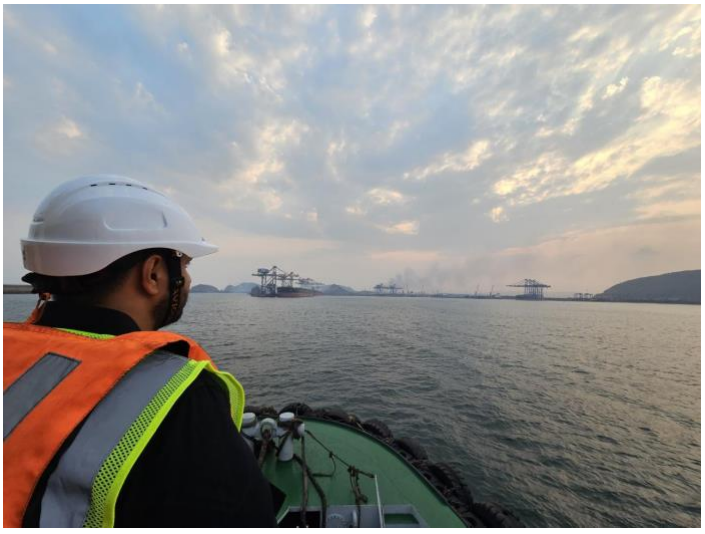
- **Energy infrastructure as strategic asset:** Production facilities, pipelines, and shipping routes are now directly linked to geopolitical stability

- **Operational continuity under pressure:** Systems must remain functional despite physical disruption, cyber intrusion, or regulatory volatility

- **Digital-physical convergence risk:** Increasing integration of AI and automation expands both efficiency and attack surface

Recent research highlights the scale of exposure. Rystad Energy estimates that over $200 billion in upstream investment is concentrated in geopolitically sensitive regions, while cyber incidents targeting oil and gas infrastructure continue to rise year-on-year.

This shifts the focus from production capacity to operational resilience. Energy systems must not only produce; they must endure disruption.



Sumit Dubey, one of YAVA's Founding Partners, observing the impact of geopolitical disruption on oil and gas infrastructure.

Copyright © 2026

Related Topics

- Europe accelerates IRIS² secure satellite network to strengthen sovereign communications (SpaceNews)
- Gartner forecasts LEO satellite communications spending to exceed $14 billion by 2026 (Gartner)
- India advances plans for assured access to space amid rising strategic competition (Defence Watch)
- Satellite operators expand hybrid connectivity services across aviation and maritime sectors (Via Satellite)
- Russia launches first rocket from restored Baikonur pad, underscoring the strategic importance of sovereign launch infrastructure (Reuters)
- Europe's first LEO navigation satellites prepare for launch as ESA expands resilient orbital capability (Space.com)
- FCC chair criticises Amazon's satellite launch pace as competition intensifies in LEO communications infrastructure (Investing.com)

Assured access to orbit and the next layer of resilient connectivity

Satellite infrastructure is entering a new phase: from commercial expansion to strategic capability. As outlined in YAVA's recent collaboration with Astraius, the ability to access orbit reliably is becoming a defining factor in infrastructure resilience.

Satellite systems now underpin communications, navigation, surveillance, and operational coordination across energy, transport, and defence systems. As these dependencies grow, so does the importance of assured and sovereign launch capability — particularly in environments where disruption is expected rather than exceptional.

March developments reinforce this shift. Investment in satellite communications and launch readiness continues to accelerate, with operators and governments prioritising secure, resilient space-based infrastructure.

The Astraius perspective reflects a broader strategic reality: future conflicts and infrastructure disruption may not begin on land or at sea, but in orbit — where communications, intelligence, and operational continuity are increasingly determined.

This shift is shaping deployment strategy across regions:

- **Assured access to orbit as strategic requirement:** Dependence on a limited number of launch providers creates concentration risk for infrastructure systems and national capabilities

- **Space as contested operational domain:** Satellite infrastructure is increasingly exposed to interference, disruption, and geopolitical competition

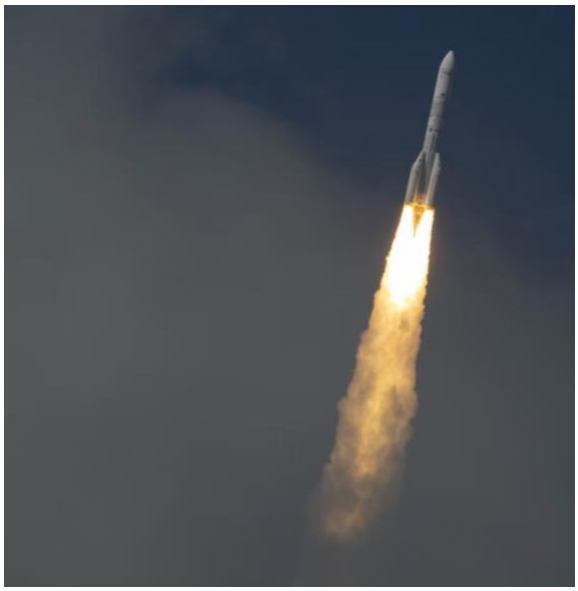
- **Integration into hybrid architectures:** Satellite systems are now embedded within terrestrial networks, supporting resilient communications across energy, logistics, and defence environments

GLOBAL DEPLOYMENT IN ACTION

According to Gartner, global spending on LEO satellite communications services is projected to reach $14.8 billion in 2026, reflecting the transition of satellite systems into core infrastructure layers.

In practice, this is where deployment capability becomes critical. Infrastructure resilience increasingly depends on the ability to integrate orbital and terrestrial systems into unified, secure architectures that can operate under pressure.

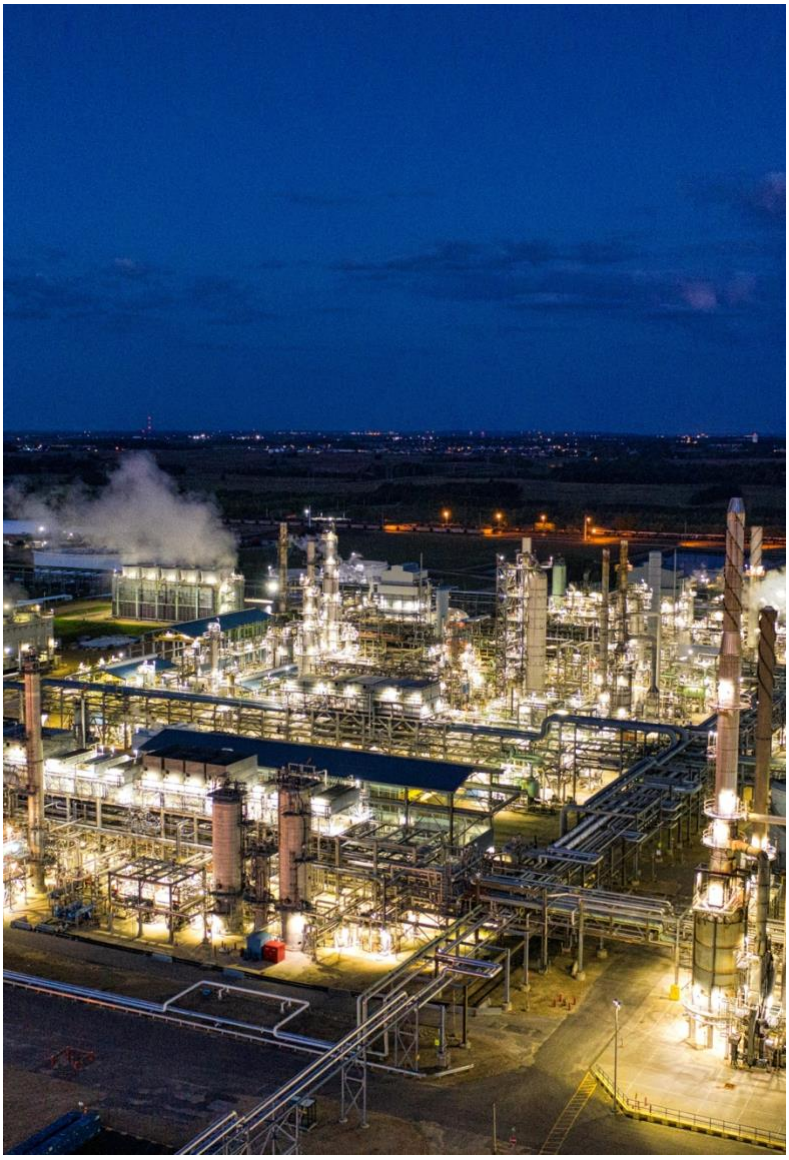
YAVA's work sits directly at this intersection, supporting governments and operators with hybrid connectivity, secure communications, and multi-region deployment capability in environments where infrastructure must remain functional despite disruption.



Rocket launches and assured access to orbit are becoming critical to national infrastructure resilience, enabling secure communications, surveillance, and operational continuity across defence and civilian systems.

Image source: European Space Agency

Copyright © 2026



Building the next generation of resilient infrastructure through secure communications, strategic partnerships and hybrid connectivity across energy, transport, and digital systems

Yet exposure is increasing alongside investment. Infrastructure is becoming more capable but also more vulnerable.

In this environment, partnerships become critical.

No single operator controls the full resilience stack. Governments, energy companies, satellite providers, telecom networks, and technology platforms are increasingly interdependent. The ability to coordinate across these systems will define infrastructure performance.

YAVA's focus remains consistent: integrating secure communications, hybrid connectivity, and engineering capability into infrastructure systems designed to operate under pressure.

As geopolitical risk becomes more visible, resilience becomes a competitive and strategic advantage.

The opportunity ahead is not simply infrastructure expansion. It is coordinated, secure systems capable of operating through disruption.

LOOKING AHEAD: PARTNERSHIPS & GROWTH OPPORTUNITIES

Infrastructure resilience in an era of geopolitical competition

March developments have reinforced a central reality: infrastructure resilience is increasingly shaped by geopolitical competition, technological convergence, and system interdependence.

Energy corridors, satellite systems, and digital infrastructure are no longer separate domains. They are interconnected layers within a single operational environment, where disruption in one system can cascade across others.

Capital investment continues to scale. Energy infrastructure, satellite networks, and AI-driven systems are all expanding rapidly.

YAVA's Event Calender

- **Black Hat Asia**
  Singapore | 21–24 April| Link
- **Innovation Zero World Congress**
  London, UK | 28–29 April| Link
- **RSA Conference 2026**
  San Francisco, USA | 4–7 May| Link
- **Gartner IT Infrastructure, Operations & Cloud Strategies Conference**
  London, UK | 16–17 Nov| 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