YAVA MONTHLY REPORT

DATE: 30.06.2026

ISSUE NO. 20

INSIDE THIS ISSUE

PG. 2-3
Maritime security: The new threat picture

PG. 4
Infrastructure security trends and technology highlight

PG. 5
Data centre resilience

PG. 6
Global deployment in action: Turning intelligence into operational response

PG. 7
Partnerships, resilience, and market outlook



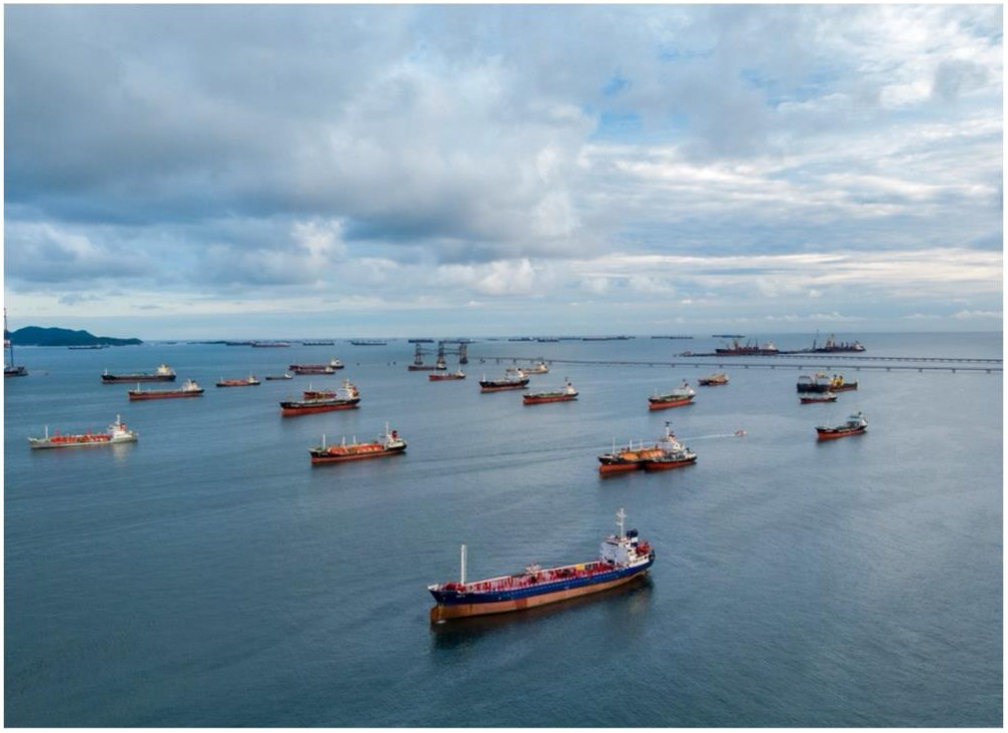
Image credit: Benoit Tessier/Reuters

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)

Copyright © 2026



Tankers waiting offshore reflect the new maritime security reality outlined by YAVA and SF Group: vessels, ports and operators now face a faster-moving threat picture shaped by contested routes, live intelligence, insurance pressure and the need for coordinated response before disruption escalates.

Image credit: Getty Images

War and Geopolitical Developments

▪ **Hormuz remains on a 60-day clock:** June's maritime picture was shaped by a ceasefire process that paused, rather than resolved, the US-Israel-Iran conflict. After renewed Israel-Iran strikes, a memorandum of understanding created a 60-day window to negotiate a final settlement.

▪ **Diplomacy keeps routing risk unstable:** Iran later warned that Hormuz could close again, while talks were delayed by renewed fighting and unresolved disputes over Lebanon, inspections and implementation. The result is a partial reopening that can reverse quickly.

▪ **Maritime risk linked to geopolitics:** Depressed transit numbers and shifting war-risk terms are downstream of this unresolved process. For operators, Hormuz remains a live diplomatic, insurance and routing risk for shipping and energy markets globally.

MARITIME SECURITY

The new threat picture demands more than traditional approaches

Why traditional security models are falling short: The maritime security environment has changed faster than many operating models.

This was the central message in YAVA's recently published article with SF Group, featuring SF Group Maritime Analyst Shane Wall, which examined how the Red Sea, Strait of Hormuz, Indian Ocean and maritime cyber domains are now converging into a single operating problem.

The foundations of maritime security have been tested severely over the past two years. Red Sea disruption has shown how a non-state actor can impose major costs on global shipping. The Strait of Hormuz has shown how maritime geography can be used as an instrument of state coercion.

The Indian Ocean has shown how traffic rerouting can move vessels into areas where piracy risk is again elevated. Cyber risk adds another layer, with vessel systems, port operations, cargo management and communications increasingly exposed to digital disruption.

The YAVA and SF Group partnership is built around this reality.

SF Group brings specialist risk management, maritime security, live intelligence and operational judgement through its SF BREATHE platform.

YAVA brings the engineering and systems integration capability needed to make that intelligence scalable, usable, and connected to the systems that clients rely on in the field.

This combination addresses a clear gap in the market. Periodic written reports, static route assumptions, and fixed escalation plans were not designed for environments that change by the hour. Operators now need live intelligence, contextual analysis, and the ability to convert information into practical decisions across routing, communications, insurance, security posture, and local response.

Three shifts are becoming increasing visible:

▪ **Checkpoints are now active operating environments:** The Red Sea, Strait of Hormuz, and Indian Ocean are live operating variables that affect cost, insurance, routing, fuel availability, and security planning.

▪ **Intelligence must be continuous:** The threat does not pause. A report produced on

Copyright © 2026

Related Topics

- **India orders agencies to be on alert after strikes on ships in the Gulf:** India's response shows how maritime disruption quickly becomes a national coordination issue when seafarers, energy flows and commercial interests are exposed (Reuters)

- **Three Indian-flagged oil tankers clear Strait of Hormuz:** The safe transit of three Indian-flagged tankers carrying more than 860,000 metric tons of oil highlights both the importance of coordinated state support and the fragility of energy lifelines (Reuters)

- **The maritime chokepoints that could be worse than Hormuz:** Recent analysis places Hormuz within a wider set of chokepoint vulnerabilities, from Taiwan to Panama, showing why maritime resilience cannot be limited to one corridor (Chatham House)

- **Oil Market Report — June 2026**: The IEA's June report provides the most current energy-market view of Hormuz disruption, supply losses and the conditions required for gradual normalisation (IEA)

- **15 countries adopt the Mombasa Declaration to fight illegal fishing**: The agreement strengthens the case for transparency, vessel tracking and data sharing across maritime security and ocean governance (AP News)



Maritime intelligence is most valuable when it moves beyond static reporting and supports live operational decisions, connecting vessel tracking, threat monitoring and coordinated response.

Friday may be out of date by Monday. In volatile marine environments, intelligence needs to move from periodic briefing to live operational support.

- **Technology is the bridge between awareness and action:** The value in making intelligence usable at the point where decisions are taken, whether that means adjusting a route, changing an escalation threshold, updating crew guidance or coordinating support across ports and local partners.

FROM STATIC REPORTING TO LIVE OPERATIONAL INTELLIGENCE

Where YAVA and SF Group fit in

The YAVA and SF Group partnership is built around a clear operating gap: clients in high-risk environments need intelligence they can act on, and the technical infrastructure to make that intelligence usable across multiple locations, teams and time zones.

SF Group brings operational security expertise, maritime intelligence, risk assessment, emergency support and on-the-ground reach. Its SF BREATHE platform is designed to provide live intelligence in environments where the threat picture does not pause for weekends, reporting cycles or board meetings.

YAVA brings the technology and engineering layer required to make that intelligence scalable. This includes software platforms, systems integration, cybersecurity, data systems, secure communications, surveillance infrastructure and support for complex operating environments where connectivity, vendor coordination and maintenance can be difficult.

The combined capability matters because the threat picture is increasingly both physical and digital. A vessel may face surface threats, drone activity, piracy risk, insurance constraints, satellite or AIS disruption, and cyber exposure across port and logistics systems. Each domain affects the other.

In the first 72 hours, a credible response should establish context, assess current threat conditions and identify likely next developments.

Over 30 days, that assessment should become a living operating picture: updated, tested and linked to decision-making. Over time, it should support a sustained posture across routing, communications, escalation, insurance, security and technical continuity.

This is the practical value of the partnership. Intelligence becomes useful when it changes decisions. Technology becomes valuable when it connects people, systems and data under pressure.

For maritime operators, offshore companies, port authorities and organisations exposed to the Gulf, East Africa or South Asia, the priority is not more information. It is better operational judgement, delivered in time to matter, through systems that can function in the environments where risk is actually unfolding.

This supports:

- Faster understanding of current threat conditions
- Better route, transit and escalation decisions
- Stronger coordination between security, logistics and technical teams
- Improved evidence for insurers, clients and stakeholders
- More resilient operating models across contested maritime environments

Copyright © 2026



Navigation resilience is becoming critical for protecting infrastructure from GPS disruption, cyber risk and fast-moving threats.

Image credit: Shutterstock

INFRASTRUCTURE SECURITY TRENDS TO WATCH

▪ **Critical infrastructure cyber risk is becoming a state-linked threat picture:** In June, the UK National Cyber Security Centre said more than 200 cyber incidents affecting UK critical national infrastructure and supporting systems had been managed in the year to May 2026, with around 75% believed to be linked to hostile state actors. For infrastructure operators, this reinforces the need to treat cyber resilience as an operational continuity issue, not only an IT risk.

▪ **Europe tests rail and maritime cyber crisis response:** ENISA's Cyber Europe 2026 exercise, held on 10-11 June, focused on large-scale cyber incidents affecting interconnected transportation systems, including rail and maritime networks. The exercise brought together more than 5,000 participants and tested coordination across technical, operational and political levels.

▪ **Civilian drone threats move beyond the battlefield:** Reuters reported in June that drone incursions at airports and strikes on oil fields are accelerating demand for counter-drone systems across airports, energy, shipping, data centres, hotels and other civil infrastructure. The trend shows how low-cost aerial threats are moving into civilian operating environments.

▪ **State-linked attacks on control systems move cyber risk into operational continuity:** A joint US advisory warned that Iranian-affiliated actors are exploiting internet-facing operational technology, including Rockwell Automation/Allen-Bradley programmable logic controllers, across critical infrastructure sectors. For operators in water, energy, government and industrial environments, the lesson is clear: exposed PLCs, weak segmentation and limited OT visibility can turn cyber activity into real-world disruption.

TECHNOLOGY HIGHLIGHT: WHEN NAVIGATION BECOMES RISK

Why signal disruption is now an infra resilience issue

The most visible infrastructure risk in June was not just the movement of drone and cyber threats into civilian environments. It was the growing disruption of navigation itself.

GPS and GNSS jamming and spoofing are increasingly affecting shipping, aviation and infrastructure operators that depend on accurate positioning, navigation and timing. What began as a conflict-zone tactic to misdirect drones and missiles is now creating operational consequences for vessels, aircraft, ports, logistics hubs, energy sites and other critical infrastructure.

This matters because navigation signals are no longer isolated technical inputs. They support vessel routing, aviation safety, cargo tracking, emergency response, remote monitoring, secure communications and time-sensitive digital systems. When signals are disrupted, the impact can move quickly from technical interference to operational delay, safety risk and continuity pressure.

The scale is now operational, not anecdotal. In June, reporting highlighted mass interference affecting more than 1,100 commercial vessels in Gulf waters in a single 24-hour period, with aviation also facing daily disruption from jamming and spoofing. For operators moving through exposed maritime and air corridors, route planning now needs to account for signal interference alongside physical security, insurance, weather and geopolitical risk.

Where YAVA fits: Secure communications, navigation resilience and OT integration are core YAVA capabilities. PNT resilience is one engineering answer to maritime, aviation, and counter-drone risk, helping operators maintain continuity when signals, systems or routes come under pressure across complex environments.

Copyright © 2026



Data centres are becoming critical infrastructure environments, where AI growth depends on resilient power, cooling, water, cybersecurity and physical protection.

Image source: SKANSKA

SPOTLIGHT: DATA CENTRES AND DIGITAL INFRASTRUCTURE RESILIENCE

When AI infrastructure becomes critical infrastructure

Data centres are no longer just digital assets. They are becoming core infrastructure environments, with direct dependencies across power, cooling, water, land use, physical security, cyber resilience, cloud connectivity and regional grid stability.

In June, the scale of this shift became more visible. Reuters reported that AI-driven demand could double data centre power and water consumption by 2030, citing UN researchers who warned that the public debate still often treats AI as software, while the underlying reality is physical infrastructure: data centres, electricity generation, cooling systems, transmission networks, chips, minerals, land and water.

This matters for infrastructure operators because data centres now sit at the intersection of digital continuity and physical resilience. A failure in power, cooling, network access or third-party facility management can affect cloud platforms, enterprise systems, public services, logistics networks, financial services, security platforms and operational technology environments.

The risk is not theoretical. In June, Google Cloud said some customer in India experienced intermittent network disruption after a fire at a third-party data centre triggered an emergency shutdown of networking equipment. The incident isolated a local point of presence in Delhi and reduced network capacity across the metropolitan area, showing how a physical incident at one facility can cascade into digital service disruption for businesses and users.

At the same time, grid operators are becoming more concerned about the behaviour of large power users. Reuters reported that large electricity users, including data centres, abruptly disconnected from the Texas grid during voltage disturbance testing. ERCOT said some groups of large power users could trigger more than 5,000 MW of demand tripping under certain fault conditions, with abrupt drops equivalent to the electricity consumption of a large city such as Boston.

Three structural implications are becoming clearer:

- Data centres are energy infrastructure customers and infrastructure risks: Operators need reliable power day and night, but large, fast-changing loads can also create stress for grids. Resilience planning must account for both sides of that relationship.

- Physical incidents can become cloud incidents: Fire, cooling failure, power shutdown or access disruption at a single facility can affect applications, websites, internal systems and customer-facing services. Third-party data centre resilience is now part of enterprise continuity planning.

- AI growth is increasing pressure on local infrastructure: Data centre development is placing growing strain on electricity grids, water supplies and communities. In June, mayors from 40 cities, including London, Phoenix and Melbourne, backed a Global Urban Data Centres Pact to guide planning, clean energy use, water efficiency and local integration.

Two relevant statistics:

- Reuters reported that data centres consumed 448 terawatt-hours of electricity globally last year, more than the whole of Saudi Arabia, with AI accounting for a fifth of the total. They also consumed 4.5 trillion litres of water and generated 189 million tons of carbon dioxide emissions

- US power demand is forecast to rise from 4,195 billion kWh in 2025 to 4,271 billion kWh in 2026 and 4,397 billion kWh in 2027, according to the EIA, with Reuters reporting that the increase is being driven by AI-hungry data centres and electrification

Copyright © 2026

Related Topics

▪ **AI data centres expand into drought-hit regions:** A Guardian analysis found that a majority of planned U.S. AI data centres are being built in areas already affected by severe drought, reinforcing how AI infrastructure growth is becoming a water-security issue as well as an energy challenge (The Guardian)

▪ **Liquid cooling becomes a resilience priority:** Nvidia's new AI data centre design uses liquid cooling and allows systems to run hotter, reducing dependence on traditional cooling towers. For operators, this shows how thermal management is becoming central to data centre continuity, sustainability and site selection (The Verge)

▪ **Community opposition grows around AI data centres:** Axios reports that data centres are becoming a visible focus for wider public concern about AI, with opposition linked to energy demand, water use, land impact and limited local benefit. This raises the importance of transparency, planning and stakeholder engagement (Axios)

▪ **Grid constraints affect data centre growth in Western Sydney:** Australia's transmission operator has warned that parts of Western Sydney are nearing grid-capacity limits as data centre demand rises. The story highlights why digital infrastructure growth increasingly depends on power planning, transmission capacity and regional resilience (The Australian)

Turning intelligence into operational response

June developments show that resilience is now judged by the speed and quality of operational response.

Whether the issue is a vessel moving through Hormuz, a port assessing cyber exposure, an airport reviewing drone detection, a hotel strengthening communications resilience or a manufacturer investigating supply-chain data leakage, the challenge is similar. Organisations need to understand the current risk picture, decide what action is required and implement changes across real operating environments.

For YAVA, this is where deployment capability becomes critical.

Clients in complex environments do not only need advisory outputs. They need practical support across physical, digital and operational domains. That means connecting assessment, engineering, integration, deployment, maintenance and partner coordination.

This includes:

▪ Site-level risk assessments
▪ Cyber and systems audits
▪ Physical security and access control reviews
▪ Secure communications and continuity planning
▪ Infrastructure remediation
▪ Vendor coordination and technical deployment
▪ Intelligence platform integration
▪ Ongoing monitoring, maintenance and support

The June risk picture reinforces why these workstreams need to be connected. A cyber incident may affect access control, logistics or client confidence. A drone incursion may require physical security, aviation coordination, communications protocols and legal review. A maritime disruption may affect fuel supply, insurance, crew safety, route selection and contractual obligations. A manufacturing breach may expose IP, customer data, employee information and supply-chain relationships.

GLOBAL DEPLOYMENT IN ACTION

This creates three priorities for deployment:

▪ **Faster mobilisation:** Clients need to move quickly from awareness to assessment and action.

▪ **Operational visibility:** Risk must be understood at asset level, not only through central reporting.

▪ **Coordinated delivery:** Cyber, physical security, infrastructure and logistics planning must support each other rather than compete for attention.

YAVA's role is to help close the gap between risk awareness and implementation. This means building and supporting systems that can work under pressure, in markets where infrastructure is fragmented, connectivity is variable and the external threat picture can change quickly.



On-site infrastructure assessment shows how global deployment depends on technical expertise, local coordination and the ability to turn risk intelligence into practical action in complex operating environments. Image credit: Microsoft

Copyright © 2026



Image credit: Getty Images

Trusted growth depends on coordinated systems, verified resilience, and partners able to support continuity across fragmented markets.

For asset owners, the priority is continuity. For insurers, it is evidence. For investors, it is confidence that infrastructure can withstand disruption. For governments, it is the stability of systems that support trade, mobility, security and public trust.

This is creating demand for more coordinated resilience models across:

- Ports, logistics and commercial asset operators
- Hotels and hospitality groups in complex markets
- Insurers, brokers and risk engineering specialists
- Cyber, physical security and infrastructure teams
- Regional partners with local deployment capability
- Technology providers and operational support networks
- Maritime intelligence and security partners

For YAVA, the direction of travel is clear. Growth will come from combining engineering capability, risk intelligence, partner expertise and implementation support into practical delivery models.

LOOKING AHEAD: PARTNERSHIPS & GROWTH OPPORTUNITIES

Trusted growth in uncertain markets

June 2026 has reinforced a central theme for YAVA: resilience is no longer judged by whether an organisation has plans, controls or reports. It is judged by whether people, systems and partners can continue operating when disruption happens.

The pressure is coming from multiple directions. Maritime routes are exposed to state coercion, non-state actors and insurance uncertainty. Critical infrastructure is facing state-linked cyber activity. Civilian sites are reviewing drone detection and response. Ports and logistics corridors are becoming strategic operating environments. Manufacturers are seeing supply-chain cyber incidents move into customer and IP exposure.

YAVA's Event Calender

- **Gartner Security and Risk Management Summit**
  National Harbour, USA | 14-16 Jun | Link
- **Understanding Global Risk Forum**
  Abu Dhabi, UAE | 19-23 Oct | Link
- **Gartner IT Infrastructure, Operations & Cloud Strategies Conference**
  London, UK | 16–17 Nov | Link
- **International Security Expo**
  London, UK | 2-3 Dec | 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