YAVA MONTHLY REPORT



DATE: 28.05.2026

ISSUE NO. 19

INSIDE THIS ISSUE

PG. 2-3
Beyond hospitality: Running hotels in complex environments

PG. 4
Infrastructure security trends and technology highlight

PG. 5
Ports and logistics resilience

PG. 6
Global deployment in action: Expanding delivery capability

PG. 7
Partnerships, resilience, and market outlook

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



A hotel explosion in Havana, caused by a gas leak, shows why hospitality assets need infrastructure-grade resilience, with safety systems, communications and emergency response able to function under sudden pressure.

Image source: Alexandre Meneghini/Reuters

War and Geopolitical Developments

▪ **Hormuz tensions sharpen energy and shipping risk:** Rising pressure around the Strait of Hormuz has reinforced the vulnerability of global energy flows, with operators reassessing vessel routing, fuel supply, insurance exposure and contingency planning across Gulf-linked trade.

▪ **Middle East conflict expands cyber and infrastructure exposure:** Regional escalation has been accompanied by increased cyber activity against banks, aviation, logistics and telecoms, highlighting how modern conflict can affect organisations through digital systems, cloud platforms and third-party dependencies.

▪ **Security risks spread across commercial and hospitality assets:** Recent incidents involving hotels and urban commercial sites show how conflict and political violence can affect assets beyond traditional military or gov operations.

BEYOND HOSPITALITY

Why operating hotels in complex environments requires infrastructure-grade resilience

Across the hospitality industry, a gap is widening between how hotels are described and how they actually perform under pressure.

In higher-risk markets, hotels are not simply hospitality assets. They function as operational infrastructure environments, with critical dependencies across power supply, access control, communications, payment platforms, medical response, and security. These systems must work reliably not only on a quiet afternoon, but during a power failure, a cyber incident, a civil disturbance, or a medical emergency at two in the morning.

Guest experience depends almost entirely on invisible systems working well. When those systems fail, the consequences are immediate, expensive, and in some environments, very hard to reverse.

This is the central challenge of operating in complex environments. The risk surface is wider. The data is thinner. The support infrastructure is more fragile. And the declared risk profile that owners, operators, and insurers rely on often does not reflect actual conditions on the ground.

The 2026 World Travel and Tourism Council's report is clear that recovery speed depends on operational preparedness; properties with stronger integrated systems recover faster than those relying on policy documents alone. The report identifies four resilience pillars: restoring traveller confidence, maintaining business continuity, ensuring decisive institutional response, and driving long-term structural adaptation.

The cyber dimension is particularly acute. According to VikingCloud and the Retail and Hospitality ISAC, 82% of North American hotels suffered a successful cyber breach in the past year, with more than half targeted five or more times. Property management systems, point-of-sale terminals, payment platforms, and vendor access portals frequently share infrastructure; creating wide and poorly monitored attack surfaces. In complex operating environments, where IT maturity is lower and support response times are longer, these vulnerabilities are harder to manage and faster to exploit.

Three structural dynamics are becoming increasingly visible:

▪ **Hospitality assets as critical operating environments:** In complex markets, a 200-room hotel operates at a comparable level of infrastructure dependency to a small-scale critical facility. Power, water, data, access control, and communications must function continuously. Failure in one system cascades to others.

Copyright © 2026

Related Topics

- **Washington Hilton attack spotlights hotel security pressures:** An attack at the Washington Hilton during the White House Correspondents' Association dinner has renewed attention on the hotel sector's long-running challenge: improving screening and protective security without undermining the guest experience (Reuters)

- **Baghdad hotel drone strike highlights hospitality exposure in conflict zones:** A drone hit the Al-Rasheed Hotel in Baghdad's Green Zone in March, with no casualties reported. The incident underlines how hotels near diplomatic, government, or strategic sites can become exposed to wider conflict dynamics (Reuters)

- **Beirut hotel strike shows risk to urban hospitality assets:** An Israeli strike on the Ramada Plaza hotel in Beirut marked the first time in the war that Israel's bombing campaign had struck the city centre, an area with restaurants and hotels (UK Gov)

- **Hormuz disruption continues to affect LNG movement:** A second Qatari LNG tanker was moving through the Strait of Hormuz to Pakistan amid the Iran conflict, using an Iranian-approved route (Reuters)

- **UK deploys destroyer as Gulf shipping risks intensify:** The UK has sent HMS Dragon to the Middle East as tensions around the Strait of Hormuz raise concern over the security of critical shipping routes. The deployment shows how maritime disruption is becoming a government-level resilience issue, with trade, energy movement and regional stability increasingly linked (BBC)



Hotel resilience depends on integrated systems, clear coordination, and tested response under pressure.

- **Risk visibility as commercial value:** The Marsh Global Insurance Market Index Q1 2026 confirms that clients with strong, verifiable risk profiles are best positioned to negotiate improved terms and enhanced coverage. The quality of evidence presented at renewal is increasingly the decisive factor.

- **Resilience as guest safety and asset protection:** Physical security, cyber risk management, power redundancy, and crisis response are not back-office concerns. They are fundamental to the guest experience and the commercial performance of the asset.

YAVA's developing risk intelligence model reflects this operating reality. The aim is to move from declared risk to observed, verified risk — through on-site technical assessment, cyber and physical systems reviews, remediation planning, and ongoing support. The focus is not on compliance documentation. It is on whether systems can actually function when they are needed.

FROM GUEST EXPERIENCE TO OPERATIONAL CONTROL

Where YAVA fits in

Hotels in complex markets frequently have policies in place. Security procedures exist. IT systems have been installed. Insurance cover has been arranged.

The gap is rarely in documentation. It is in integration. When systems were procured from different vendors, installed at different times, and maintained by different parties, or not maintained at all, they are unlikely to function together under pressure. A power failure disable the access control system.

A security incident may find that communications tools, response procedures, and escalation routes have not been tested together.

This is what makes resilience in complex operating environments a practical engineering problem. The question is not whether controls exist on paper. It is whether systems, people, and procedures can perform when needed.

YAVA operates across this gap: on-site technical assessment across cyber, physical, and infrastructure systems; access control and systems integration; secure communications and power resilience review; crisis response readiness; technical remediation; and ongoing support through annual maintanence and re-assessment.

Our strategic partnerships extend this capability into risk intelligence, insurance advisory, travel risk management, crisis management, and medical response coordination. For hotel operators, owners, and insurers working across higher-risk markets, this combination of engineering-led assessment and insurance-aligned advisory creates a stronger evidence base, better insurability outcomes, and faster response coordination when incidents occur.

Together this supports:

- Improved risk visibility and verified operational evidence
- Better insurability and stronger terms at renewal
- Stronger guest and asset protection
- Operational continuity through integrated system and teting procudures

For YAVA, the objective is to turn resilience from a static assurance exercise into a practical operating capability. By connecting assessment, remediation, partner coordination and ongoing support, hotels can move beyond policy compliance and build systems that are better prepared to perform under real-world pressure.

Copyright © 2026



Image source: Corey Payne/USA/Rex/Shutterstock

AI in military drones is redefining national defence strategies by accelerating surveillance, targeting and response capabilities.

INFRASTRUCTURE SECURITY TRENDS TO WATCH

Hybrid threats continue to reshape exposure

▪ **CISA urges infrastructure outage planning:** The US Cybersecurity and Infrastructure Security Agency has launched a formal programme urging water utilities, transport operators, and other critical infrastructure organisations to plan for geopolitical crisis scenarios where communications, cloud, and technology services may be severed (Federal News Network)

▪**Third-party access remains a major weakness:** IBM X-Force Threat Intelligence Index 2026 reports a fourfold increase in major supply chain and third-party breaches over five years. Hotels, logistics operators, and infrastructure assets with fragmented vendor ecosystems face the sharpest exposure (IBM)

▪**Middle East logistics shifts toward resilience:** Middle Eastern governments are accelerating new overland and rail-sea corridor proposals to reduce dependence on Strait of Hormuz and Red Sea maritime routes. For operators across energy, hospitality, and logistics, this signals a structural shift in how regional supply chains and asset operations are planned (South China Morning Post)

▪ **Insurance evidence is now the decisive factor at renewal:** Marsh's Global Insurance Market Index Q1 2026 records a fifth consecutive quarter of rate competition but risk quality determines outcomes. Clients with documented, verifiable operational controls are securing materially better coverage. Those without are not (Marsh)

TECHNOLOGY HIGHLIGHT: AI, CONFLICT AND INFRA RISK

When warfare becomes the threat intelligence case study

The Middle East conflict has produced the first large-scale documented test of AI-enabled cyber warfare in an active conflict zone and the lessons for infrastructure operators are direct.

Across the conflict, AI tools were used to generate highly convincing phishing campaigns at scale, create fraudulent emergency applications designed to harvest sensitive location and identity data, and accelerate reconnaissance across exposed networks and devices. Iranian-aligned groups deployed AI-assisted attacks against energy companies, financial institutions, aviation systems, and government infrastructure across the Gulf and beyond. According to WEF analysis, the conflict demonstrated how geopolitical instability and armed conflict are directly reshaping the cyber threat landscape — and how geographic distance provides no reliable defence.

The AWS data centre strike also exposed a gap that AI-based risk models had not adequately anticipated: when kinetic military action physically destroys cloud infrastructure, the resulting service disruption may fall between a traditional property policy and a cyber policy, both of which increasingly carry war-risk exclusions. Lloyd's of London is reported to be reassessing cloud infrastructure risk modelling and pricing in response.

The operational takeaway is consistent with YAVA's wider risk intelligence model: AI tools improve detection and response capability but only where the underlying operational infrastructure is sound. In environments where systems are fragmented, vendor access is poorly governed, and backups are untested, AI adds a layer of analytical output over unresolved underlying exposure. Used well, it supports resilience. Used on a weak foundation, it creates false confidence.

Copyright © 2026



Ports and logistics infrastructure are becoming frontline resilience assets, as disruption around Hormuz and the Red Sea drives a structural shift toward alternative trade corridors and multimodal supply routes.

Image source: AFP

SPOTLIGHT: PORTS AND LOGISTICS RESILIENCE

When trade corridors become risk environments

Ports and logistics infrastructure rarely feature in hospitality or hotel risk conversations. In May 2026, they should.

Disruption to the Strait of Hormuz and continued pressure on Red Sea shipping lanes have triggered one of the most significant structural shifts in global trade logistics in a generation. Middle Eastern governments, led by Saudi Arabia, the UAE, and Turkey, are urgently developing new overland and rail-sea corridor proposals to create alternative trade routes that bypass exposed maritime chokepoints. Analysts are describing this as a structural reconfiguration of the region's logistics architecture, moving away from dependence on vulnerable maritime infrastructure and toward multimodal alternatives designed with resilience in mind.

This matters to infrastructure operators well beyond shipping. When trade corridors are disrupted, the effects move through fuel availability, food supply, construction materials, hotel consumables, and guest transport. Hotels and hospitality assets in affected regions are not isolated from these pressures; they sit downstream of the same disrupted supply chains.

The IEA has confirmed that Middle East conflict removed close to 20% of global LNG supply from the market, disrupted Qatari export capacity, and pushed gas prices to their highest levels since 2023 across Asia and Europe. The combined effect on infrastructure-dependent operators, including hospitality assets reliant on grid power or imported fuel is direct and material.

Three structural implications for operators:

▪ **Supply chain dependency is a resilience risk:** Operators relying on single-source supply routes for fuel, consumables, or communications hardware face material operational exposure when those routes are disrupted. Buffer stock and alternative procurement are increasingly treated as Infrastructure requirements, not procurement processes.

▪ **Power and energy infrastructure is directly affected by logistics disruption:** Hotels and commercial assets dependent on grid power or imported fuel face heightened exposure during supply chain stress. Backup generation and connection to alternative power sources are becoming practical operational necessities in complex markets.

▪ **Infrastructure operators are redesigning resilience from first principles:** The acceleration of new trade corridor development across the Middle East illustrates a wider principle: where existing infrastructure is assessed as insufficiently resilient, investment flows into new routes rather than simply reinforcing old ones. The same logic applies to hotel and hospitality asset operations.

Two relevant statistics:

▪ The Strait of Hormuz accounts for approximately one-third of global seaborne trade in fertiliser, around 40% of global helium supply, and approximately 15% of global polyethylene capacity. Disruption here is a global supply chain event, not a regional one.

▪ Egypt recorded Suez Canal activity growth of 23.6% in Q3 of the 2025/26 fiscal year as shipping was partially rerouted through the Red Sea and Suez corridor, while international energy companies committed over $19 billion in new investment to Egypt's energy sector. Infrastructure positioned near alternative trade corridors is seeing accelerated commercial activity.



As pressure on Hormuz and Red Sea routes increases, ports and logistics corridors are becoming critical resilience assets for operators in shipping and beyond.

Copyright © 2026

Related Topics

- **Oil market recovery could be delayed into 2027:** Aramco's CEO warns that continued disruption through the Strait of Hormuz could delay oil market recovery into 2027 (Reuters)

- **UK deploys warship with potential Hormuz mission in mind:** The UK had deployed HMS Dragon to the Middle East, with a possible role linked to Hormuz security (Reuters)

- **Global chokepoint vulnerability:** The Middle East conflict exposes the vulnerability of global chokepoints, with implications for maritime routes, supply chains and sectors dependent on secure trade flows (World Economic Forum)

- **Bunker fuel shortages create new pressure on shipping:** Disruption linked to the Iran war is affecting bunker fuel supply, with shipping companies slowing vessels, revising schedules and looking at alternative fuels (AP News)

GLOBAL DEPLOYMENT IN ACTION

Operational resilience across ports, hotels, and high-risk infrastructure

As geopolitical disruption, physical security threats and supply chain volatility continue to converge, global deployment is becoming less about entering new markets and more about maintaining operational continuity across exposed environments.

For YAVA, this creates a clear delivery challenge: clients do not only need to understand risk. They need the ability to act quickly across multiple locations, asset types and operating conditions.

This is especially relevant across ports, logistics hubs, hotels, commercial assets and critical infrastructure sites. These environments are increasingly connected through shared dependencies: power, communications, access control, digital systems, transport routes, local security, insurance requirements and regulatory oversight.

A disruption in one layer can quickly affect the wider operating environment. A port delay can create inventory pressure. A hotel security incident can affect confidence, insurance and business continuity. A communications outage can undermine incident response. A regional conflict can change routing, fuel availability and asset exposure almost overnight.

YAVA's deployment model is designed around this reality. The focus is on connecting risk intelligence with practical implementation across physical, digital and operational domains.

This includes:

- Site-level risk assessments
- Cyber and systems audits
- Physical security and access control reviews
- Communications and continuity planning
- Infrastructure remediation
- Vendor coordination and technical deployment
- Ongoing monitoring and support

The value of this approach lies in execution. In complex markets, resilience cannot depend on advisory outputs alone. It requires trusted delivery routes, local understanding, technical capability and the ability to coordinate multiple workstreams under pressure.

Three priorities are becoming increasingly important:

- **Faster mobilisation:** Clients need support that can move from assessment to action quickly.
- **Operational visibility:** Risk must be understood at asset level, not only through central reporting.
- **Coordinated delivery:** Physical security, cyber, infrastructure and logistics planning must work together rather than separately.

This reflects a wider shift in the market. Organisations are no longer asking whether risks exist. They are asking whether their assets, systems and partners can continue operating when disruption happens.

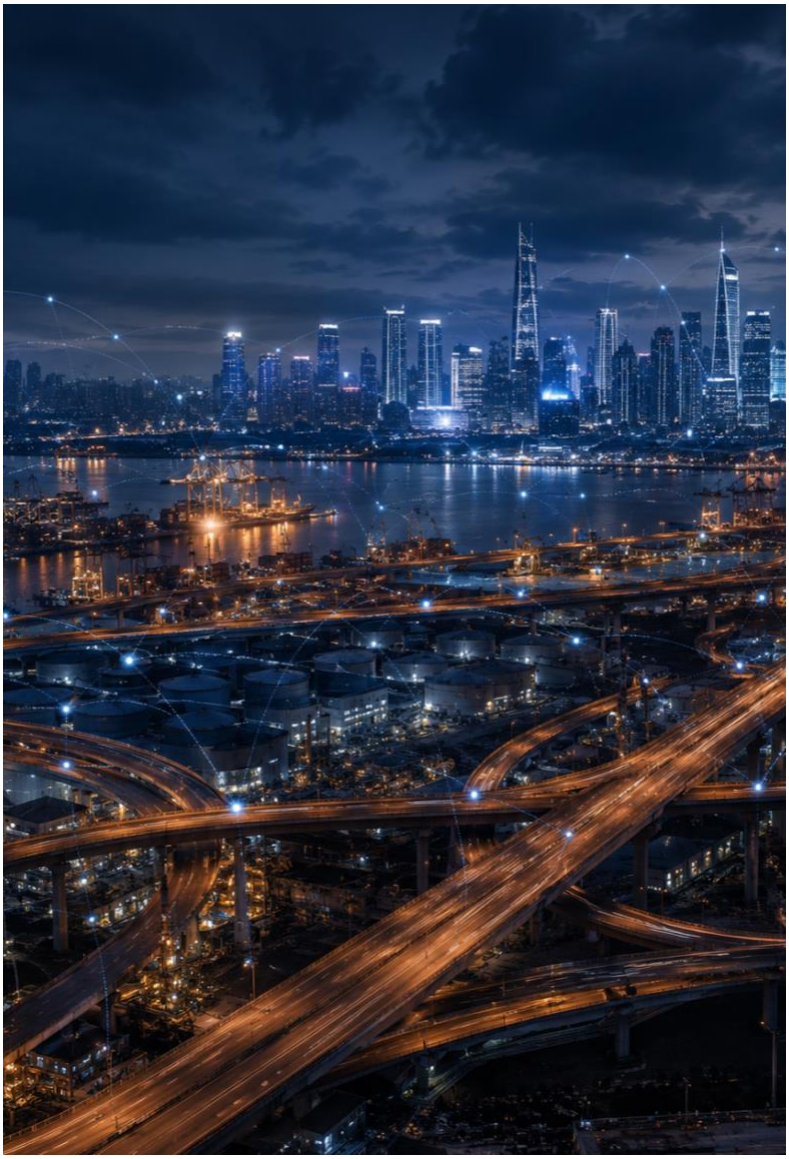
For YAVA, global deployment means helping clients close the gap between risk awareness and real-world resilience.

This is where deployment capability becomes critical: combining local presence, technical expertise and trusted partners to turn resilience from planning into operational action.



Destroyed civilian infrastructure shows how disruption in one layer can quickly affect power, communications, transport access and operational continuity across exposed environments.

Copyright © 2026



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

A maritime disruption can affect fuel, ports and supply chains. A cyber incident can interrupt aviation, hospitality and financial services. A physical security threat can quickly become a commercial, reputational and insurance issue. This is changing how resilience is valued. Organisations are not only asking whether they are exposed to risk. They are asking whether they have the partners, systems and technical capability to respond when conditions deteriorate.

This is creating demand for more coordinated resilience models across:

- Hospitality, logistics and commercial asset operators
- Insurers and risk engineering specialists
- Cyber, physical security and infrastructure teams
- Regional partners with local deployment capability
- Technology providers and operational support networks

For YAVA, this reinforces a clear direction of travel: connecting risk intelligence, engineering capability, physical security and implementation support into practical delivery models.

LOOKING AHEAD: PARTNERSHIPS & GROWTH OPPORTUNITIES

Trusted growth in uncertain markets

May 2026 developments show that resilience is now being judged by performance under pressure, not by policy, planning or declared controls alone.

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.

Recent events across the Middle East have made this more visible. Conflict, cyber activity, logistics disruption and pressure on energy routes are no longer separate risk categories. They interact across shared infrastructure.

YAVA's Event Calender

- **Gartner Security and Risk Management Summit**
  National Harbour, USA | 9–1 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