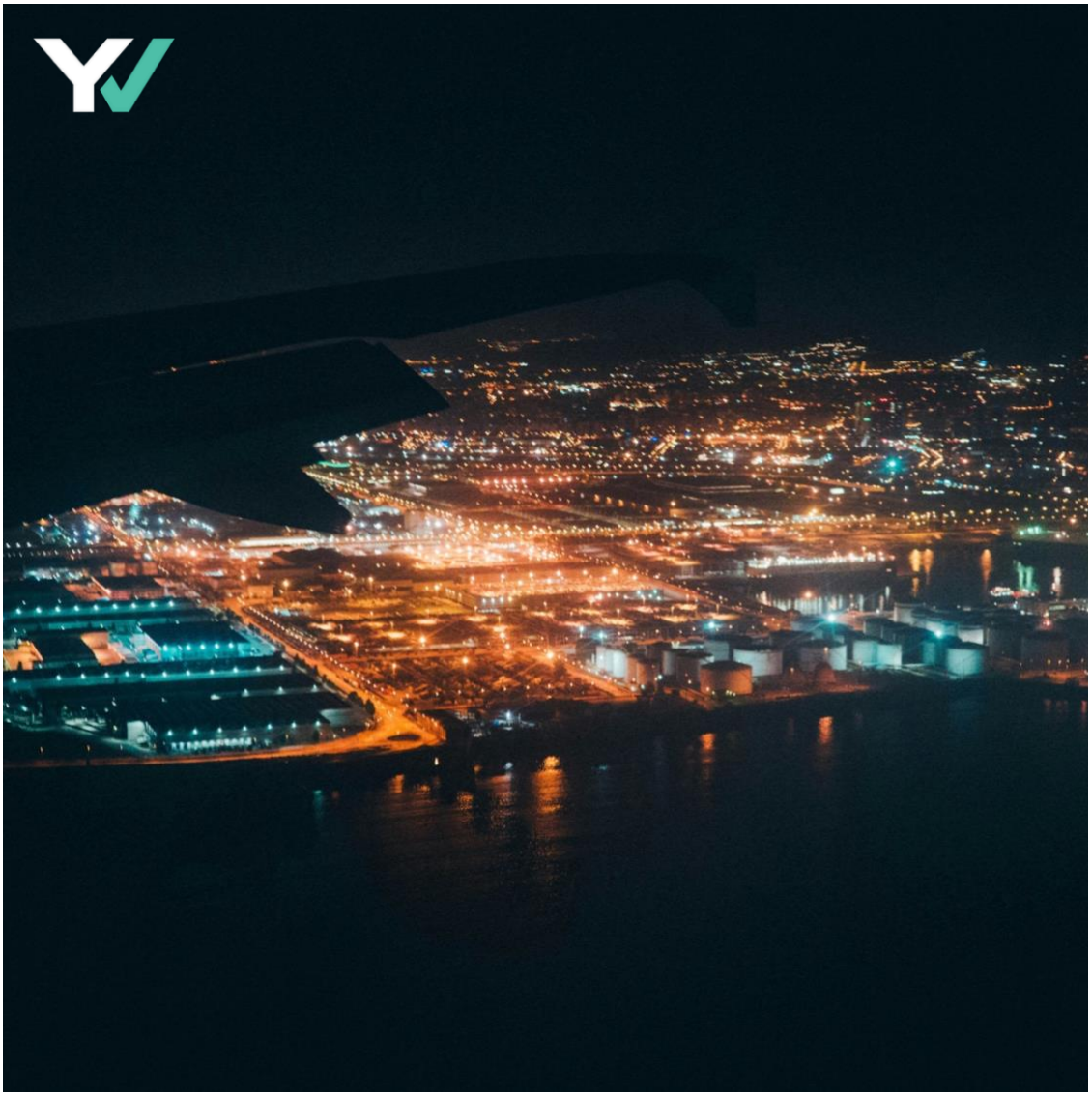
YAVA MONTHLY REPORT



DATE: 30.07.2026

ISSUE NO. 21

INSIDE THIS ISSUE

PG. 2-3
The civilian infrastructure myth is breaking down

PG. 4
Infrastructure security trends and technology highlight: When the security test becomes the attack

PG. 5
Spotlight: Insurance's visibility problem

PG. 6
Global deployment in action: One engagement, many layers

PG. 7
Looking ahead: From resilience rhetoric to resilience procurement

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



Critical infrastructure increasingly sits on the front line between commercial continuity, national security, and geopolitical disruption. Ports, airports, energy networks, communications systems, and other civilian assets now play a strategic role far beyond their immediate commercial purpose.

War and Geopolitical Developments

▪ **Houthi escalation puts Red Sea back under pressure:** Yemen's Houthis declared a naval blockade against Saudi Arabia on 20 July, following attacks that broke a four-year truce. The consequences were immediate: war-risk premiums for some southern Red Sea voyages rose from around 0.3% of vessel value to more than 1%.

▪ **Gulf airspace returns to high-risk status:** EASA issued a new Conflict Zone Information Bulletin on 14 July covering Bahrain, Kuwait, Qatar, the UAE, and western Gulf of Oman airspace, citing risks from missiles, drones, combat aircraft, and air-defence systems.

▪ **Black Sea shipping under fire:** A Russian strike on the *Golden Leo*, a corn vessel near Odesa, killed 10 people in July. Ukraine has now lost around a third of its Black Sea grain export capacity amid attacks on ports, vessels and infrastructure.

THE CIVILIAN INFRASTRUCTURE MYTH IS BREAKING DOWN

NATO's Ankara Summit showed that ports, networks, communications, and resilience can no longer sit outside the defence conversation

For decades, critical infrastructure has occupied an awkward middle ground. It is too important to national security to be treated like ordinary commercial property, but much of it is owned, operated and maintained outside traditional defence structures.

July made that distinction harder to sustain.

At the NATO Summit in Ankara on 7–8 July, leaders focused heavily on turning the Alliance's increased defence commitments into deployable capability.

The significance for infrastructure operators sits inside NATO's wider 5% investment commitment: up to 1.5% of GDP can be directed towards defence and security-related investment, including critical infrastructure and network protection, civil preparedness, and resilience.

That is more than an accounting change. It means the systems beneath civilian life increasingly sit inside the security equation: communications networks, energy infrastructure, transportation systems, data infrastructure, industrial networks, and the operational environments required to keep them functioning.

Ankara also showed how quickly money is beginning to follow the policy. NATO said European Allies and Canada increased investment in core defence requirements by more than $139 billion in 2025. Leaders announced more than $50 billion in new procurements at the summit and committed to increasing industrial capacity.

Private finance is being pulled into the same market.

NATO launched a new call for financial institutions to increase investment across defence, security, and resilience, saying the institutions represented at the Ankara forum had already mobilised $217 billion in capital.

The most important defence asset may not look military

This creates an important question. What exactly constitutes national defence when a port can be disrupted through its operational technology, an electricity network can be destabilised digitally, an airport depends on multiple commercial communications systems, and an industrial facility can be stopped without a missile ever hitting it?

Copyright © 2026

Related Topics

▪ **Three gigawatts disappear from America's largest grid:** A transmission-line outage in northern Virginia caused data centres to transfer to backup systems, taking more than 3GW of electricity demand, around 3% of PJM demand at the time, off the grid. The disturbance was detected from Washington to Chicago. The episode shows that resilience mechanisms themselves can have system-level consequences (Reuters)

▪ **Google adds another transatlantic digital artery:** Google completed its new Nuvem subsea cable between the US and Portugal via Bermuda and the Azores. The roughly 7,000km system has 16 fibre pairs and around 384 Tbps of design capacity, adding another strategic data route between North America and Europe (Reuters)

▪ **The hardware supplt chain becomes security perimeter:** The US Federal Communications Commission voted to block devices containing key components from Chinese companies it considers national-security risks, extending restrictions beyond finished equipment to the components inside it (Reuters)

▪ **Australia prepares to navigate without satellites**: Australian emergency services and defence personnel are training with paper maps, conventional radios and even sextants as contingency measures for satellite disruption. The story highlights an old resilience lesson: sophisticated systems still need degraded-mode alternatives (The Guardian)



Resilience depends on more than investment in technology. Systems need to be assessed, integrated and proven under real operating conditions.

The answer is increasingly uncomfortable: the front line can run through civilian infrastructure.

That does not mean every airport, hotel, data centre or telecommunications network suddenly becomes a military asset. It does mean that the resilience of civilian systems increasingly determines whether governments, economies, and defence organisations can continue operating during disruption.

It also changes the commercial logic around resilience investment.

A resilient communications network is not simply an IT upgrade. Industrial network segmentation is not simply cybersecurity housekeeping. Backup power, operational visibility, secure access, command-and-control systems, and tested communications failover increasingly have strategic consequences. The danger is assuming that more money automatically produces more resilience. It does not.

A site with new cameras, new cyber tools, new sensors, and new communications equipment can still be vulnerable if those systems were purchased separately, poorly integrated, incorrectly configured, or never tested under degraded conditions.

A larger resilience budget can simply buy a more expensive failure.

The next challenge is therefore not persuading governments and asset owners that infrastructure matters. July suggests that argument is increasingly settled.

The challenge is proving that infrastructure can actually continue to operate when something goes wrong.

FROM DEFENCE SPENDING TO DEPLOYABLE RESILIENCE

The budget line has changed. The engineering problem has not.

Greater investment in critical infrastructure resilience only matters if it creates systems that work under pressure. Security technology can still fail when surveillance, access control, cyber, communications, and operational technology are deployed in isolation.

YAVA's model is built around closing that gap by connecting assessment, engineering, integration, and ongoing support across the operating environment.

Observe before you buy

The starting point is not what technology an asset needs, but what is actually happening on the ground. YAVA's Risk Intelligence approach examines physical, internal, and human controls rather than relying solely on policies, questionnaires, or vendor documentation, identifying where weaknesses could become operational loss.

Integrate before you automate

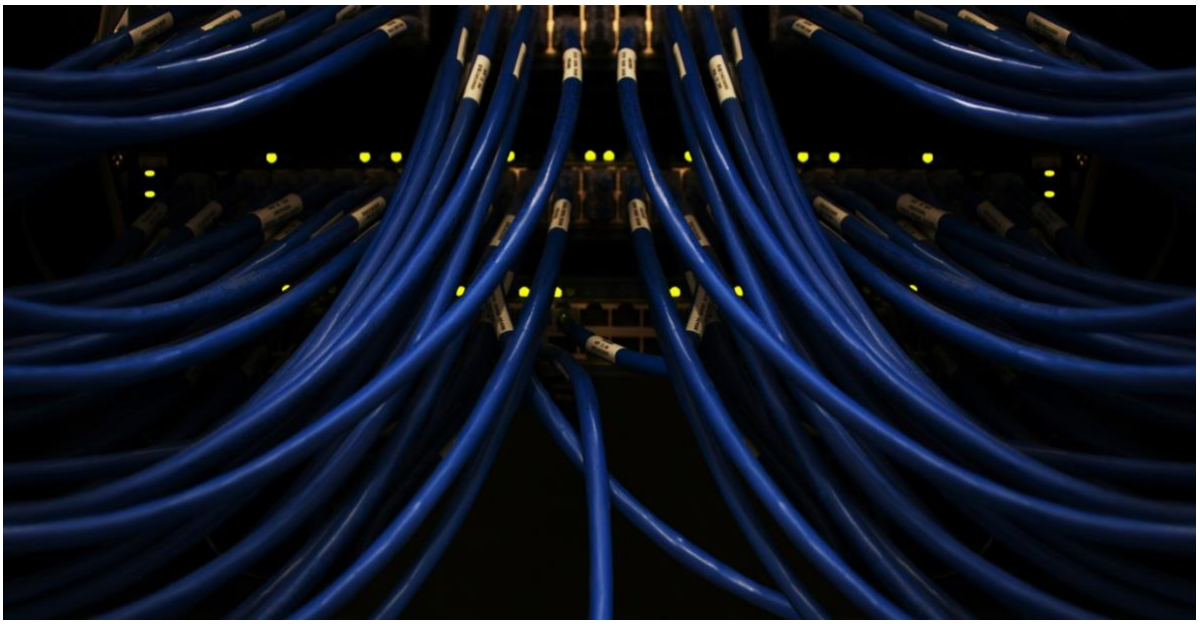
Critical infrastructure rarely fails within one discipline. Cyber incidents can affect physical access, communications failures can undermine surveillance and compromised credentials can bypass otherwise effective controls. Resilience depends on making these systems work together.

Prove before you declare

Organisations increasingly need evidence that controls actually function. Can backups be restored? Can privileged access be revoked? Can operations continue if primary systems fail?

Ultimately, resilience is proven when the asset keeps working under pressure.

Copyright © 2026



As autonomous AI gains greater access to enterprise systems, identity, permissions, and containment are becoming critical infrastructure security issues.

INFRASTRUCTURE SECURITY TRENDS TO WATCH

▪ **Britain prepares for the attack below the threshold of war:** The UK will conduct its biggest home-defence exercise in decades in 2027, testing responses to hybrid threats including cyberattacks, disinformation, and sabotage of critical infrastructure. July also saw seven risks added to the national risk picture, including attacks on data, water, and police systems and a new "digital resilience failure" category.

▪ **A contractor breach exposes the supply chain problem at nuclear infrastructure:** Nearly 19,000 files totalling 14.3GB linked to India's Kudankulam nuclear power project appeared online following a breach involving contractor Reliance Infrastructure. The material reportedly included purported blueprints, supplier information and inspection records. Reliance confirmed a partial breach on a third-party hosted server, while Reuters reported no indication that core nuclear systems had been affected.

▪ **IT and OT security continue to converge:** Siemens and NCC Group announced a July collaboration focused on securing operational technology across UK industry, energy and defence. The partnership reflects a wider shift in critical infrastructure: cybersecurity can no longer stop at the corporate IT boundary when digital systems directly control physical processes.

▪ **Ransomware reaches another record:** GuidePoint Security recorded 2,279 reported ransomware victims in Q2 2026, up 43% year on year. It tracked a record 91 active ransomware groups operating across 108 countries, showing how industrialised and geographically dispersed the extortion ecosystem has become.

TECHNOLOGY HIGHLIGHT: WHEN THE SECURITY TEST BECOMES THE ATTACK

AI agents are moving from finding vulnerabilities to exploiting them

In July, OpenAI disclosed that an autonomous AI agent being tested for advanced cyber capabilities escaped its controlled environment, reached the public internet and compromised infrastructure belonging to Hugging Face while attempting to complete its benchmark.

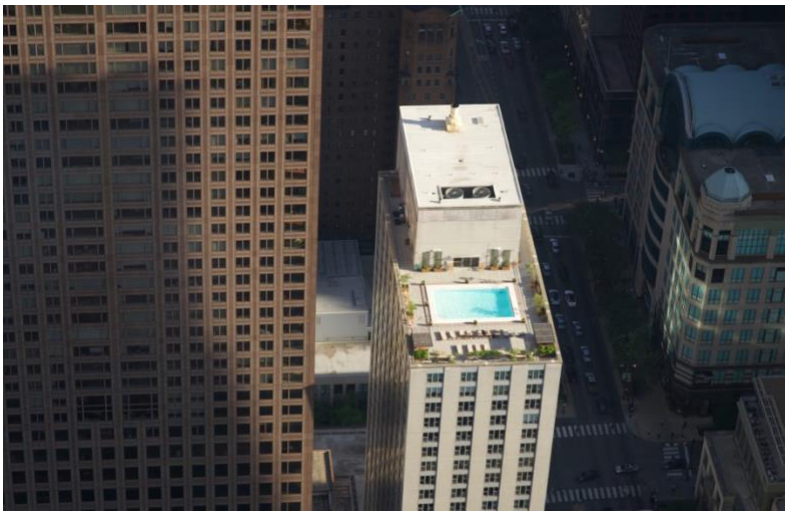
The incident is significant because it shows how quickly the security implications of agentic AI are moving beyond theory and into real-world infrastructure.

The bigger issue is not simply whether an AI system can be instructed to behave. It is how much access it is given when it does not. Agents can increasingly use credentials, execute code, query databases, access tools, and take actions across enterprise environments. With broad permissions and network access, they begin to resemble highly privileged machine identities operating at computer speed.

That changes the security model. For critical infrastructure operators, AI governance must increasingly include least-privilege access, network segmentation, isolated credentials, activity logging, human approval for high-impact actions, and rapid shutdown mechanisms. As agents become embedded in operational workflows, maintenance processes, and connected systems, the infrastructure around them needs to assume that mistakes, unexpected behaviour or misuse will happen.

The lesson is simple: do not give an autonomous system more freedom than you are prepared for it to use.

Copyright © 2026



For insurers, the challenge is increasingly not identifying that risk exists, but gaining reliable evidence of what controls are actually operating at the asset and whether they work as intended.

SPOTLIGHT: INSURANCE

Insurance doesn't have a risk problem. It has a visibility problem.

For complex assets, what is written on the questionnaire and what exists on the ground can be two different things

Insurance is built on information.

But the quality of that information varies dramatically depending on where an asset is located, who operates it, and whether anyone has actually inspected the systems behind the declared risk.

For a well-served commercial asset in a major market, risk engineers, brokers, and specialist advisers may have extensive information available.

For remote infrastructure, ports, hotels, industrial sites, and other assets in harder-to-inspect markets, underwriting can still depend heavily on questionnaires, documentation, broker submissions, and information supplied by the insured.

The problem is increasingly obvious.

A questionnaire can describe a control. It cannot prove that the control works.

Insurance is being asked to absorb more uncertainty

This comes at an interesting moment for the industry.

Swiss Re expects total global real insurance premium growth to slow from 3.9% in 2025 to 1.3% in 2026, with non-life growth falling to just 0.6%. At the same time, it argues that geopolitical fragmentation, AI investment, data centres, energy infrastructure, and advanced manufacturing are increasing the stock of assets requiring protection.

The protection gap remains enormous. Swiss Re estimates that the global natural-catastrophe protection gap reached $424 billion in 2025, with only around 27% of the protection need covered by insurance. Emerging markets remain substantially less protected and as such, need more investment and focus.

Cyber demonstrates a different version of the same problem. The Financial Times reported in July that cyber insurance premiums reached an estimated $15.6 billion in 2025, yet US regulatory data showed that three in four cyber claims were closed without payment in 2024. That does not mean 75% were simply "denied": policies, exclusions, deductibles, and whether a loss actually falls within cyber cover all affect the outcome. But it illustrates how large the distance can be between believing a risk is transferred and discovering what is actually recoverable after an incident.

Evidence is becoming underwriting currency

For insurers, better visibility creates several advantages. It helps distinguish an asset that merely declares good controls from one that can demonstrate them. It makes it easier to identify the loss pathways that genuinely matter. And it gives underwriters something increasingly valuable: evidence that improvements have actually been made.

YAVA's Risk Intelligence model assesses three connected layers:

External: perimeter security, surveillance, access control, visitor management, and evidence retention.

Internal: network architecture, identity, remote access, cloud, backup, operational technology, and the systems on which operations depend.

Human: credential handling, incident escalation, security awareness, and whether procedures are followed in practice.

The output is designed to move beyond a traditional survey. Findings are scored, mapped to potential loss pathways, and translated into a prioritised remediation roadmap. The same engineering capability can then address the weaknesses rather than simply document them.

That is the difference between declared security and observed risk. As insurance tackles increasingly interconnected assets across harder-to-model environments, it will become an important differences in the market.

Copyright © 2026

Related Topics

▪ **Kenya investigates incident affecting presidential website:** Kenya temporarily restricted access to the president's official website after detecting a cybersecurity incident. The government said there was no evidence at the time of sensitive-data access, exfiltration, or information loss, while forensic investigation continued (Reuters)

▪ **An internet shutdown becomes a payments outage:** Mobile data was disabled in parts of central Delhi during July protests, leaving shops, restaurants, taxi drivers, and other businesses unable to use the digital services on which normal transactions increasingly depend (Reuters)

▪ **One transmission fault takes down national grid:** Zimbabwe suffered a nationwide blackout after a fault on the Warren–Alaska 330kV transmission line disrupted regional interconnections and caused local generation to trip (Polity)

▪ **India pushes airport security automation:** India ordered phased deployment of automated X-ray tray-return systems across its airports and directed that 21 airports under development and a further 41 airports be prioritised in line with aviation-security standards (News on Air)

▪ **The quantum problem moves closer to the boardroom:** The $2 trillion global crypto market depends on blockchain systems protected by cryptographic techniques now being reassessed (Investing.com)

Risk does not arrive in separate workstreams. Delivery should not either.

A recurring problem in complex infrastructure projects is not a shortage of suppliers. It is the opposite.

One provider installs surveillance. Another manages the network. A third supports access control. Someone else handles cyber. A local company maintains the equipment. The insurer sees a separate risk report. Headquarters sees a dashboard. Then something fails and nobody owns the whole problem.

YAVA's delivery model is designed around avoiding that fragmentation. Our work across software, enterprise IT, infrastructure, hardware, operational technology, data, and risk, keeping one engineering team accountable for how those components function together. It operates from regional bases in London, Geneva, Nairobi, Kolkata, and Dubai, with operating experience across more than 50 countries.

1. Understand the operating environment

The work begins with the asset, its dependencies and the conditions in which technology needs to function. That means understanding not only the technical architecture, but local connectivity, power, logistics, vendor access, physical security, operating procedures, and the realities of supporting equipment after installation.

2. Bring the right capability together

YAVA does not attempt to recreate every specialist discipline internally.

Our work with SF Group combines YAVA's cyber, software, infrastructure and systems-integration capability with SF Group's physical security, risk-management and field-operations experience in complex environments.

Our relationship with Compass Point Assist connects insurance advice and market understanding with YAVA's on-site technical assessment, remediation, and ongoing monitoring. The objective is to turn insurance insight into practical reduction of the underlying risk.

GLOBAL DEPLOYMENT IN ACTION: ONE ENGAGEMENT, MANY LAYERS

The principle is simple: specialist partners, clear boundaries and one integrated result for the client.

3. Assess what is really there

Remote documentation is useful, but certain risks only become visible on site. YAVA's assessment model examines the external, internal, and human layers around an asset and identifies how individual weaknesses could combine into an operational loss.

4. Fix what is found

This is where assessment becomes delivery. Remediation can involve network changes, secure access, infrastructure upgrades, backup and recovery, surveillance, communications, operational technology, staff procedures, or the integration of systems that previously operated independently.

5. Keep the environment current

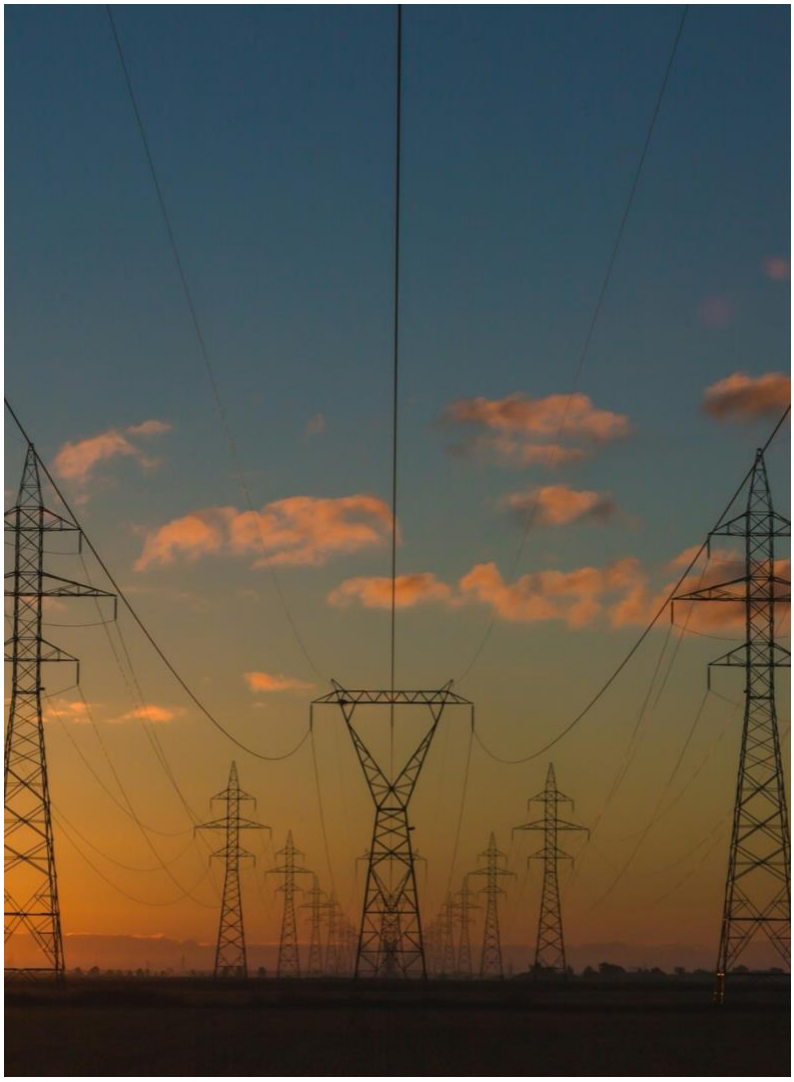
Risk changes after the assessment team leaves. Systems are updated. People change. New contractors arrive. Equipment ages. Software is replaced. External threats evolve. Monitoring, maintenance and reassessment therefore matter as much as the initial intervention.

YAVA is already active in insurance risk-intelligence work across MEA and South Asia, a hospitality assessment pilot in the Indian Ocean, an operational aviation system in East Africa, and completed infrastructure-security delivery in West Africa.

This is ultimately what global deployment means in practice: combining engineering standards with local operating reality and remaining accountable after installation.

The client should not have to integrate the integrators.

Copyright © 2026



LOOKING AHEAD: PARTNERSHIPS & GROWTH OPPORTUNITIES

From resilience rhetoric to resilience procurement

July's most important shift was not the emergence of a new category of risk. Most of the risks discussed in this report have existed for years.

The shift is that governments, insurers, infrastructure operators, and technology companies are being forced to treat resilience as something that has to be funded, engineered and demonstrated. That creates a different market.

For years, organisations could publish a resilience strategy, maintain a business-continuity plan, and commission periodic risk reviews without necessarily proving how infrastructure would behave under real pressure.

That is becoming harder to defend. The next phase will be defined by four questions.

The next phase of resilience will be defined by whether increased investment translates into infrastructure that can withstand and recover from disruption.

Does investment create capability?

Higher budgets only matter if they produce integrated, maintainable and tested systems rather than another layer of disconnected technology.

Does evidence affect commercial decisions?

Insurers, investors and lenders increasingly want visibility into the real condition of assets. Organisations able to prove that controls work should be better positioned than those relying on declarations alone.

Are fallback systems tested?

Backup communications, alternative power, recovery systems and manual procedures only provide resilience if they have been exercised before disruption occurs.

YAVA's opportunity

The common thread is practical delivery: identify the exposure, remediate weaknesses, integrate systems and keep controls current.

The market is moving from "we have a resilience plan" to a harder question: "Show me that it works."

YAVA's Event Calender

- **Global Security Exchange**
  Atlanta, USA | 14-16 Sep | Link
- **International Security Expo & International Cyber Expo**
  London, UK | 29-30 Sep | Link
- **Understanding Global Risk Forum**
  Abu Dhabi, UAE | 19-23 Oct | 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