CRISIS24

GLOBAL RISK FORECAST 2026

FUTURE READY, NOW.

Grimes Canyon Road in California at dusk.

TABLE OF CONTENTS

GLOBAL RISK FORECAST 2026

Aerial view of Paulista Avenue in São Paulo, Brazil.

Foreword

The Global Risk Forecast is our annual outlook for security and resilience leaders, assessing global risk to support the protection of people and operations in the year ahead. Crisis24's intelligence team translates complex signals into insights that you can use to make better, faster decisions. As state competition re-intensifies under the evolving new world order, the impact of crises will accelerate and amplify across digital and physical domains. Yet, with foresight and disciplined execution, today's risks can become tomorrow's advantages.

That reality underpins this year's report theme: Future Ready, Now.

This forecast draws on our 24/7 global network and artificial intelligence (AI)-enabled analysts' skills at identifying trends, anticipating threats, and offering informed "next moves." Along with regional expertise bolstered by an unparalleled on-the-ground network, their specialized disciplines span cybersecurity, aviation, maritime, environment, health, and protective intelligence so that they can offer insightful risk assessments and resilience recommendations. In a world defined by uncertainty, readiness remains our – and your – advantage.

Mick Sharp
Senior Vice President, Operations & Intelligence
Crisis24

Sally Llewellyn
Vice President, Global Intelligence
Crisis24

Two dynamics shape the year ahead:

A POLARIZED, TRANSACTIONAL WORLD AMPLIFIES GEOPOLITICAL VOLATILITY.

Persistent policy divergence – most visible in US-European approaches to Russia – creates uncertainty and openings for opportunistic rivals. In Asia, an assertive Beijing and a less-consistent Washington raise miscalculation risks at sea and along disputed borders, where even brief standoffs can jolt logistics and markets. In the Middle East and the Horn of Africa, local politics and proxy competition will drive volatility as the danger of sudden protests, conflict, and violence threatens foreign interests. Across the Americas and parts of Africa, drones, automation, and AI are scaling organized crime, while polarization deepens divides. Extreme weather will compound risk management pressures, further compressing timelines for crisis response.

TECHNOLOGY MULTIPLIES RISK AND OPPORTUNITY AS ADVERSARIES ADOPT AND ADAPT AT PACE.

Technology is no longer just a tool, but an accelerant reshaping competition and exposure. With shifting alliances and rapid adoption by state and non-state actors, technology is both an arena – e.g., China and the US scaling for AI advantage – and a weapon. As risk teams deploy new tools to enhance foresight, detection, and resilience, they also widen exposure to manipulation and disruption. AI and data abundance are redefining how human judgment and machine insight combine to enable operations. Advantage favors those who read signals sooner, operationalize decisions faster, and manage risk while spotting opportunity.

Together, these themes define a world that is faster, more connected, and harder to predict. The challenge – and opportunity – for organizations is to turn awareness into advantage. The Global Risk Forecast distills the signals that matter, helping leaders anticipate disruption and act decisively to strengthen resilience and protect people and operations – even in the most demanding physical and virtual environments.

Executive Summary

The coming year will be defined by change. Evolving trade policies, shifting allegiances, rapid advances in technology, and persistent global crises will create an operating environment that is fast-moving and hard to predict. Organizations should expect episodic shocks, but the most significant challenge will be near-continuous, overlapping incidents that test resilience, decision-making, and trust.

The convergence of political tensions and the weaponization of technology mean short-term crises can quickly multiply. A local outage, data breach, or protest can escalate into a supply chain or reputational crisis within hours. Being "future ready" requires flexibility at every layer of operations – systems and cultures that absorb shocks, adapt in real time, and continue to move forward as conditions change.

Global stability will continue to hinge on shifts in US policy and major power competition. As Washington balances domestic politics with strategic competition, allies and rivals remain uncertain about direction and intent, producing fluctuations in trade, defense, and compliance requirements. Western policy toward Russia will remain divided, with US and European views on ending the Ukraine conflict continuing to diverge – creating friction for businesses operating across jurisdictions or considering re-entry to Russia. Similar uncertainty will extend to energy transition and technology policy, where mixed signals from major economies complicate planning and investment.

The Middle East will be reshaped in the aftermath of the Israel–Hamas war. A ceasefire pauses fighting but does not address root causes of instability. Renewed Iran-Israel hostilities would upend fragile balances and disrupt shipping routes, airspace, and regional trade. Businesses should expect volatility around diplomatic milestones, ripple protests worldwide, and shifting travel or security restrictions. Perceptions of US consistency and Israel's isolationism and military-driven approach will also influence investor confidence and government decision-making.

Across Sub-Saharan Africa, competition for influence is deepening as China, Russia, Türkiye, and Gulf States expand economic and security footprints while African governments press for greater agency. International investments bring capital but can strain governance and heighten social tensions. The Red Sea and Horn of Africa will remain critical corridors where piracy, access disputes, or renewed Ethiopia–Eritrea tension could trigger shipping delays and higher costs. In the Sahel, AI-generated misinformation is amplifying anti-Western sentiment and fueling unrest, increasing reputational and operational risk for international companies already navigating evolved militancy and complex nationalization agendas.

In Asia, miscalculation risks remain high. Tensions between Taipei and Beijing will persist, although direct confrontation is unlikely as Beijing prioritizes non-military tactics. Military build-ups, contested borders, and nationalist politics in the South China Sea and Taiwan Strait increase the chances of short-term accidental escalation. Even a brief standoff could close vital airspace or sea lanes, raising insurance costs, and causing weeks of disruption across global supply chains. Companies should prepare for rerouting, backlog management, and stronger brand-protection strategies to counter surges in online nationalism.

Across the Americas, risks are converging where technology, politics, and major events intersect. Criminal groups are integrating drones, AI, and cyber tools, blurring physical and digital threats. Polarized politics and public frustration increase the potential for targeted protests or reputational attacks on companies and executives. The 2026 FIFA World Cup will magnify these pressures as millions gather around venues, airports, and hotels across North America. Expect heightened security screening, protest activity, weather-related disruptions, and misinformation targeting event sponsors and service providers.

Technology is an enabler and amplifier of risk. AI-driven misinformation and synthetic media now spread faster than verification can respond; convincing fabrications can trigger market swings, protests, or reputational crises before the truth emerges. Organized crime is using AI to enhance extortion and evade surveillance, while law enforcement and corporate defenders race to automate detection and response. Cyber threats are shifting from opportunistic to strategic, with state-linked actors embedding themselves in critical infrastructure – including ports, energy networks, and aviation systems.

Extreme weather is now a constant operating factor. Heat waves, storms, and flooding will disrupt logistics, construction, and events throughout the year; even the World Cup may face weather-related delays and safety restrictions. Health systems remain vulnerable to misinformation and uneven vaccination coverage, leading to localized outbreaks that can prompt new restrictions or travel concerns.

A defining trend is how technology magnifies small crises into larger ones. Localized cyberattacks, viral posts, or infrastructure failures can cascade through global systems with speed and reach. AI and social media accelerate this process, turning contained incidents into broader crises that disrupt markets, supply chains, and reputations. A power failure in one region can trigger global IT impacts; a fake video can spark protests that close transport routes; a data leak can evolve into a geopolitical dispute.

Amid this complexity, advantage will depend on foresight and agility. Organizations that embed live intelligence into decision-making, clarify decision authority, and build flexible recovery mechanisms will adapt at speed – anticipating disruption, acting decisively, and protecting people and operations.

THE CONVERGENCE OF **POLITICAL TENSIONS** AND THE WEAPONIZATION OF TECHNOLOGY MEAN **SHORT-TERM CRISES CAN QUICKLY MULTIPLY.**

AI & TECHNOLOGY: DEFINING RISK TRENDS

Speeding cars on race track at night.

ARTIFICIAL INTELLIGENCE

NARRATIVES AS AN ATTACK SURFACE: THE 2026 INFORMATION RISK FORECAST

EXECUTIVE SUMMARY

In 2026, strategic risk will emerge from the information domain as narrative-driven threats. Misinformation and disinformation, executive impersonation and deepfakes, and coordinated brand attacks now move faster than corporate response cycles. These narratives can jolt markets, lead to physical threats, and erode brand equity. As brands concentrate value in executive reputation and authenticity, leadership identity becomes both an amplifier and an attack surface. As synthetic content becomes more convincing, organizations will need continuous monitoring, bespoke incident response, and cross-functional management to protect reputation, safety, and continuity – and to compress decision windows from hours to minutes.

KEY JUDGMENTS

Speed and credibility will define 2026 information risk; narrative attacks will outpace response and erode trust and value.

Executive identity will increasingly serve as both a brand amplifier and attack vector, increasing exposure to impersonation and deepfake operations.

Online-offline risks will reinforce each other, with polarizing narratives driving harassment and protest activity, while physical incidents fuel viral narratives that impact markets.

AI-enabled, authoritative-looking content forces faster, cross-functional responses linking protective intelligence with reputation management.

Man analyzing data.

Threat Landscape

In 2026, the defining feature of information risk is the combination of speed and credibility. Narrative attacks now move through authoritative-looking channels and synthetic media that appear authentic.

TECH AMPLIFIERS: COMPROMISED CHANNELS AND SYNTHETIC CONTENT

In January 2024, hackers compromised the US Securities and Exchange Commission's (SEC's) official X account to post a false approval of a Bitcoin ETF, briefly jolting crypto markets before a correction landed.

In May 2023, an AI-generated image of an explosion at the Pentagon circulated widely, triggering a short-lived market dip before verification caught up.

In 2025, fraudsters in Singapore used deepfake technology to pose as senior executives and convince a finance director to transfer USD 499,000.

INFORMATION-PHYSICAL CONVERGENCE

Polarizing narratives about pricing, access, or corporate behavior spill quickly into the physical domain. Online campaigns can escalate into harassment, doxxing, stalking, and protests at homes or offices. A single high-profile act of violence against a corporate leader is reported within minutes, attracting speculation, conspiracy, and copycat threats that strain protective-intelligence and communications teams.

Physical safety incidents – whether a workplace injury, a confrontation at a retail site, or a protest gone wrong – are captured, edited, and remixed into synthetic "evidence" that travels further than the facts.

In December 2024, following the killing of United Healthcare's executive, social channels overflowed with negative sentiment toward the insurance industry. Speculation and conspiracy narratives forced security, communications, and investor-relations teams into a prolonged information-management posture. These narratives reportedly disrupted insurance claim processing and left a lasting impact on broader insurance markets.

For organizations with executive-centric branding, leadership identity functions both as a brand amplifier and an attack surface. Protecting it now requires aligning protective intelligence with media monitoring and reputational risk management.

OUTLOOK

The decisive advantage in 2026 will go to organizations that elevate information risk to a board-level security function and embed it within enterprise resilience alongside cyber, physical security, and business continuity. Detection technology will continue to improve, but detection alone will not close the exposure. The real constraint is coordination at speed.

Even as AI-generated content becomes more realistic, companies that compress response windows from hours to minutes, demonstrating measurable control over narrative and sentiment, will protect leadership identity and safety, preserve revenue, retain talent and customers, and avoid valuation shock.

Impacts and Patterns Associated with Synthetic Content

COMPROMISED REGULATOR ACCOUNT	AI-GENERATED PENTAGON EXPLOSION IMAGE	DEEPFAKE CFO AND COLLEAGUES ON VIDEO CALL
Observed Impact Brief crypto market move	**Observed Impact** Short-lived market dip, media amplification	**Observed Impact** USD 499,000 transfer loss
Pattern Note Authority lends instant credibility	**Pattern Note** Visuals outrun verification	**Pattern Note** Timing and cultural cues defeat controls

Deepfake technology on screen.

ARTIFICIAL INTELLIGENCE

Stronger Responses Required

Organizations cannot eliminate information risk, but they can narrow exposure. Effective mitigation relies on combining rapid detection with practiced coordination, treating narrative attacks like operational crises rather than communications challenges.

MITIGATION STRATEGIES

- **Plan and Govern:** Build incident command structures for information risk and include board-level reporting as part of governance.
- **Monitor:** Conduct persistent monitoring across open sources and media signals to surface narrative risks and exposure early.
- **Decide Fast:** Exercise cross-functional protocols to make coordinated decisions within minutes, rehearsing realistic blends of information and physical risk.
- **Act:** Debunk rapidly, escalate/takedown on platforms, brief key stakeholders, and refer fraud or threats to law enforcement.

SIGNALS TO WATCH

- **Compromised authority and synthetic visuals:** Hacked regulator or corporate accounts and AI-generated crisis imagery that briefly move markets and shape early narratives.
- **Executive and finance-focused deepfakes:** Convincing impersonations on calls or video that bypass controls and enable high-value fraud.
- **Online-offline escalation:** Polarizing narratives fueling harassment, doxxing, and protests, and physical incidents remixed into synthetic "evidence" that spreads faster than facts.

RECOMMENDED ACTIONS

Program-Level Actions

- **Incident Response Planning:** Establish incident command structures tailored to information risk; assign roles and escalation authorities.
- **Board Reporting:** Integrate reporting into governance to position information risk as resilience, not just brand management.

Day-to-Day Measures

- **Persistent Monitoring:** Continuously track open sources and media signals to identify emerging narratives and exposure.
- **Swift Action:** Debunk rapidly, escalate/takedown harmful content, brief key stakeholders, and refer threats/fraud to law enforcement.

Woman reviewing code.

CYBERSECURITY

CYBER PREPOSITIONING AND THE EMERGING THREAT TO CRITICAL INFRASTRUCTURE

EXECUTIVE SUMMARY

Critical Infrastructure (CI) will be a central focus of strategic competition through 2026 and will become increasingly vulnerable to covert penetration. Cyber prepositioning – quietly embedding long-term access inside Operational Technology (OT) – will likely become routine statecraft. Adversaries will seek persistence for months or years, holding access in reserve until crisis conditions justify disruption. This marks a shift from opportunistic cybercrime toward strategic leverage. Emerging technologies, including AI and digital twins, will both strengthen defenses and expand the attack surface, raising operational and geopolitical risks for multinational companies that depend on complex supply chains and essential services.

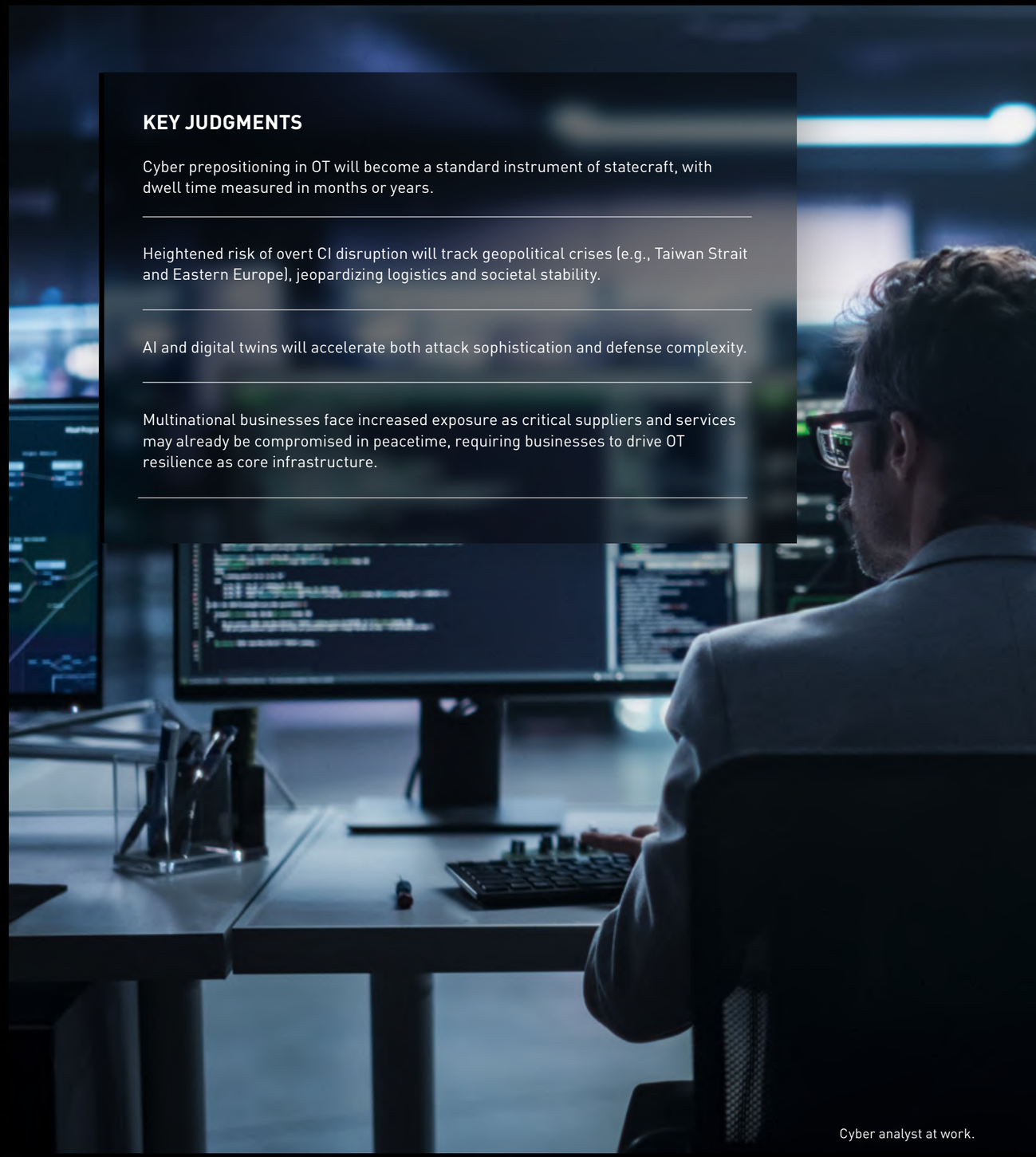
KEY JUDGMENTS

Cyber prepositioning in OT will become a standard instrument of statecraft, with dwell time measured in months or years.

Heightened risk of overt CI disruption will track geopolitical crises (e.g., Taiwan Strait and Eastern Europe), jeopardizing logistics and societal stability.

AI and digital twins will accelerate both attack sophistication and defense complexity.

Multinational businesses face increased exposure as critical suppliers and services may already be compromised in peacetime, requiring businesses to drive OT resilience as core infrastructure.



Cyber analyst at work.

Threat Landscape

CI AND OT EXPOSURE

CI comprises the essential physical and digital assets that deliver energy, transportation, water, healthcare, telecommunications, financial, and other services. OT – systems that monitor and control physical processes – has historically sat apart from the public internet, but many environments still rely on legacy software, proprietary protocols, and limited segmentation. As connectivity deepens, threat actors will find new ways to penetrate OT systems.

PREPOSITIONING AS STATECRAFT

Cyber prepositioning is the covert establishment of persistent access within OT environments of rival systems. Unlike financially motivated crime, the objective is to remain undetected for extended periods and then access during a conflict or heightened tension. This turns CI into a latent arena of coercion: a geopolitical trigger can escalate cyber access into kinetic disruption.

In 2026 and beyond, cyber prepositioning in OT systems will likely become a routine part of statecraft across the geopolitical spectrum. Threat actors will more likely use control over industrial systems, logistics operations, energy infrastructure, and communication networks to strengthen their influence without triggering open conflict. There has already been increased persistence with recent intrusions as adversaries embed themselves for months or years without being detected.

ILLUSTRATIVE CASES

Disruption to energy and utilities (power grids, pipelines, water) has immediate societal effects; breakdowns in ports, rail, airport hubs, or air traffic control can halt logistics and trade; and failures in telecoms and financial networks can degrade communications and commerce. Past incidents underscore the pattern: Russian threat actors compromised Ukraine's power grid in 2015-2016 after months inside the networks, temporarily cutting power to hundreds of thousands of people. In 2023, US authorities revealed a China-affiliated group had gained long-term access within US and Guam telecommunications.

TECHNOLOGY AMPLIFIERS

Emerging technologies will intensify both the risk and resilience of cyber prepositioning. Adversaries will likely use AI to automate persistence, blend into normal traffic, and extend dwell time without detection. Defenders will scale AI-driven anomaly detection and adopt digital twins to stress-test recovery scenarios. However, if compromised, those models can be turned against operators – revealing vulnerabilities and accelerating disruption before defensive measures can take hold.

BUSINESS EXPOSURE

By the end of the decade, major powers could routinely hold dormant access to foreign CI as a hedge. Multinationals risk operating atop already-compromised providers during peacetime, with effects that can cascade across logistics and essential services during crises.

OUTLOOK

Rising geopolitical tensions and the persistent hostile presence inside critical networks will redefine operational risk. Organizations will expand work with third-party cybersecurity partners to map potential compromise points within OT systems. CI operators are likely to grow more inward-looking as critical technologies are treated as both economic drivers and national security assets, and as regulatory demands on OT expand. Recent government moves to invest in major technology sectors point to a broader effort to work more closely with the industry to bolster supply chain resilience and strengthen OT security.

Female engineer reading code in server room.

INCIDENT PATTERNS

SECTORS MOST EXPOSED

- Energy, transport
- Telecoms
- Finance (cross-border dependencies increase leverage)

ACCESS METHOD

- Covert infiltration of OT
- Persistence measured in months/years

TRIGGER CONDITIONS

- Escalation tied to geopolitical flashpoints (e.g., Taiwan Strait, Eastern Europe)

OPERATIONAL IMPACTS

- Power/water outages
- Port/rail/airport disruption
- ATC degraded
- Financial network interference

BUSINESS EFFECTS

- Supply chain stoppages
- Service degradation
- Travel/trade delays
- Reputational and continuity risks

Stronger Responses Required

Stronger, coordinated responses are necessary as prepositioning becomes a normalized instrument of competition. The aim is to shorten dwell time, raise the cost of persistence, and preserve safe operations under pressure – without undermining safety-critical processes in OT.

MITIGATION STRATEGIES

- **Fusion-led Planning:** Integrate OT threat feeds, malware signatures, anomalous traffic, GPS-jamming reports, and supplier alerts into a single dashboard; set a strict triage window.
- **OT Environment Hardening:** Separate OT from corporate systems; maintain offline backups and reliable generator power to preserve safety operations during disruptions.
- **Vendor Assurance and Continuity:** Demand a software bill of materials (SBOM) and security attestations; pre-identify secondary suppliers for essential control systems to reduce single-point failure risk.
- **People and Finance Readiness:** Enforce MFA, conduct realistic phishing drills, and set clear region-specific operating rules; align insurance limits and pre-authorize funding to accelerate response.

SIGNALS TO WATCH

- **Evidence of persistent OT compromise:** Public/government disclosures or advisories revealing long-dwell intrusions, anomalous traffic, or segmentation bypasses in telecoms, energy, transport, finance, or water networks.
- **Emerging tech exposure:** Alerts, patches, or advisories tied to digital-twin platforms or AI-driven OT defenses that, if compromised, could be weaponized against operators.
- **Geopolitical flashpoint targeting:** Coordinated activity around the Taiwan Strait, Eastern Europe, or other contested regions that escalates pressure on logistics, ports, or air traffic control dependencies.

RECOMMENDED ACTIONS

Program-Level Actions

- Stand up an intelligence-fusion process that pulls OT threat indicators, new malware signatures, anomalous network traffic, GPS-jamming reports, and supplier alerts into one view with a defined triage window.
- Enforce separation between critical OT and corporate IT; maintain offline backups and assured generator power for key sites.
- Require SBOMs and security attestations from vendors; confirm secondary suppliers for essential control systems.
- Review cyber-insurance limits, model worst-case downtime, and pre-authorize funds for incident response teams.

Day-to-Day Measures

- Enforce multi-factor credentials; run realistic phishing drills; publish clear rules for operations in high-risk regions.
- Coordinate with third-party cybersecurity partners to map likely compromise points within OT, and validate detection coverage.

Cybersecurity engineer working on a laptop.

ENERGY & INFRASTRUCTURE

AI AND ENERGY COMPETITION LIKELY TO ELEVATE US-CHINA TENSIONS

EXECUTIVE SUMMARY

In 2026, companies in China and the US will continue developing increasingly capable, energy-intensive AI systems, driving greater strategic competition between Beijing and Washington. To power this growth, China is pairing renewables with emerging nuclear technologies, while the US contends with mounting energy-infrastructure bottlenecks. Small modular reactors (SMRs) will likely begin supplying electricity to commercial data centers in both countries from the late 2020s to early 2030s, becoming a crucial enabler that may influence which leads in AI. Scaling energy production to meet AI demand will provide opportunities, but will also heighten tensions as both countries secure uranium supply chains, develop High-Assay Low-Enriched Uranium (HALEU) capacity, and accelerate energy build-outs.

This global energy competition will intensify the international, regional, and local risks that come with strained infrastructure, displaced communities, and natural resource competition.

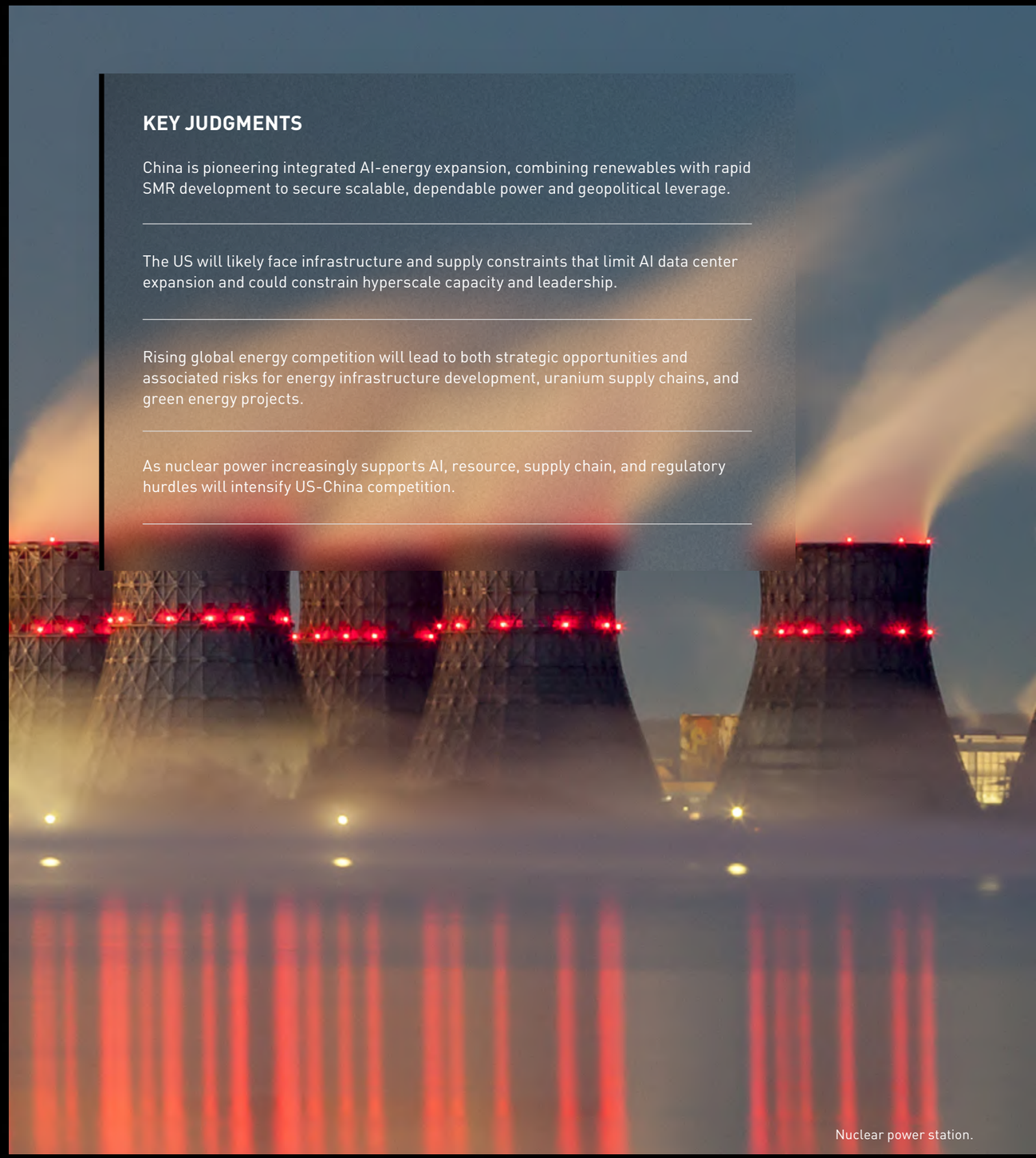
KEY JUDGMENTS

China is pioneering integrated AI-energy expansion, combining renewables with rapid SMR development to secure scalable, dependable power and geopolitical leverage.

The US will likely face infrastructure and supply constraints that limit AI data center expansion and could constrain hyperscale capacity and leadership.

Rising global energy competition will lead to both strategic opportunities and associated risks for energy infrastructure development, uranium supply chains, and green energy projects.

As nuclear power increasingly supports AI, resource, supply chain, and regulatory hurdles will intensify US-China competition.



Nuclear power station.

Threat Landscape

AI'S GROWING STRAIN ON ENERGY INFRASTRUCTURE

AI's computational hunger is accelerating global electricity demand, stressing grids designed for variable loads rather than 24/7 baseload. China's coordinated strategy couples AI growth with renewables and SMRs, improving energy security and supporting carbon goals.

China already operates commercial SMRs and is working to integrate them into its new power system, enabling operators to circumvent grid constraints, optimize costs/emissions, and harden them against geopolitical energy risks.

Commercial SMRs will likely supply electricity to data centers in China from the late 2020s. To date, the most notable commercial SMR development is the China National Nuclear Corporation's (CNNC) Linglong One. It is the first of its kind globally to pass the International Atomic Energy Agency's (IAEA) comprehensive safety review, and it generates 125 MW. Linglong One is expected to begin operation by 2026.

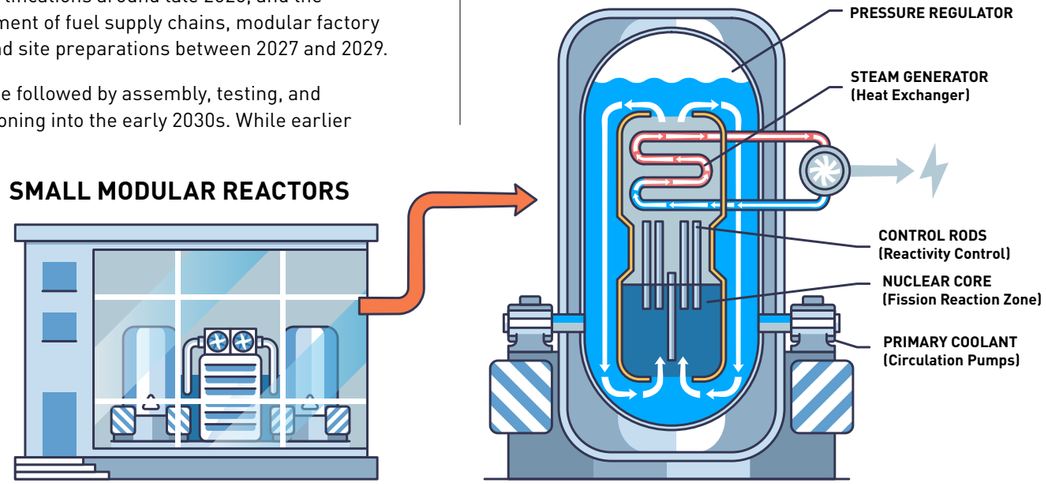
The US is pursuing projects targeting the implementation of operational SMRs by the early 2030s, with several designs currently in advanced licensing stages and construction slated to begin later this decade. In October 2025, the US and UK signed the Atlantic Partnership for Advanced Nuclear Energy agreement to accelerate reactor design approvals, streamline site licensing, and reduce barriers to investment. Key milestones will include final design certifications around late 2026, and the establishment of fuel supply chains, modular factory setups, and site preparations between 2027 and 2029.

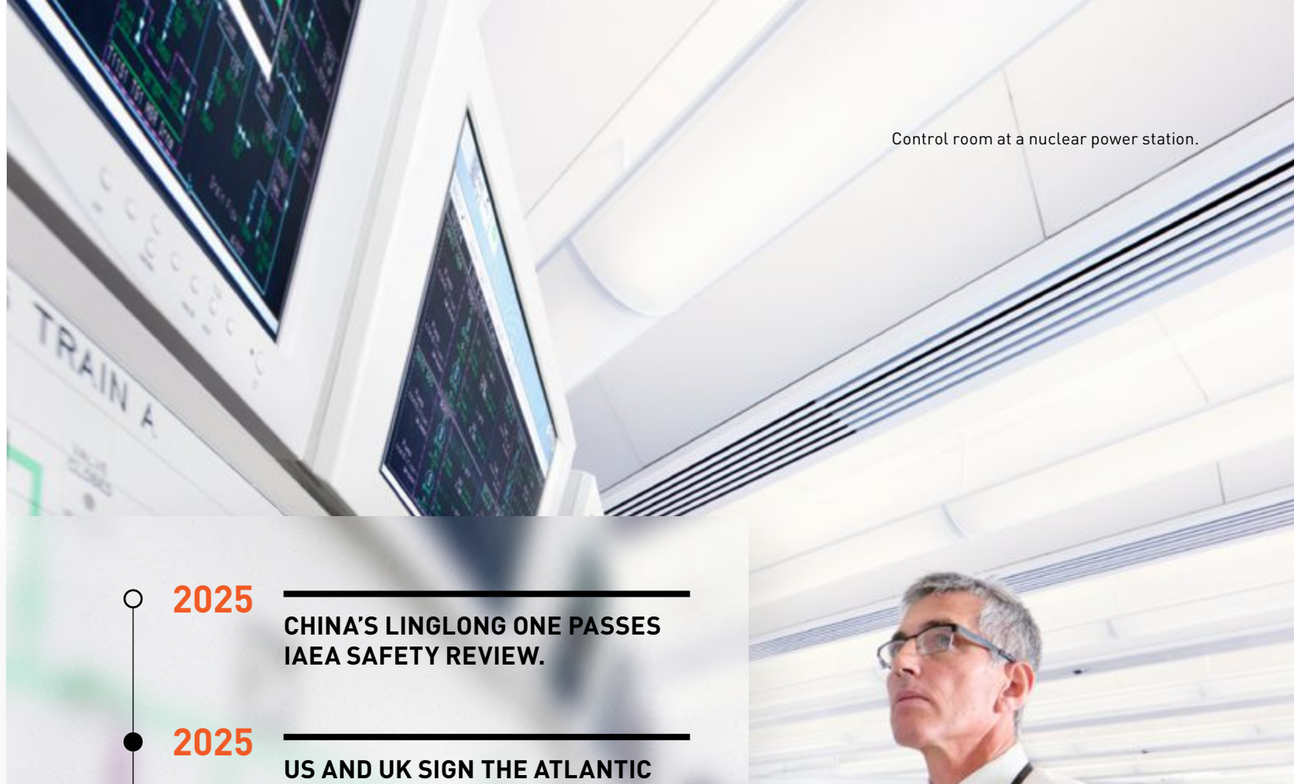
This will be followed by assembly, testing, and commissioning into the early 2030s. While earlier demonstration and microreactor units may supply niche sites from 2027-2028, full-scale SMR fleets supporting major data centers will materialize in the early 2030s.

A SOLUTION TO GROWING DEMAND

SMALL MODULAR REACTORS ARE **COMPACT, FACTORY-BUILT NUCLEAR REACTORS** (≤~300 MW) THAT CAN FLEXIBLY SCALE POWER FOR **AI DATA CENTERS**.

THEY OFFER STABLE, CARBON-FREE ELECTRICITY AND CAN BE DEPLOYED **FASTER THAN TRADITIONAL PLANTS**





Control room at a nuclear power station.

2025
CHINA'S LINGLONG ONE PASSES IAEA SAFETY REVIEW.

2025
US AND UK SIGN THE ATLANTIC PARTNERSHIP FOR ADVANCED NUCLEAR ENERGY AGREEMENT.

2026
LINGLONG ONE EXPECTED TO BEGIN OPERATIONS.

LATE **2026**
TARGET FOR US DESIGN CERTIFICATIONS.

2027 2029
US FUEL SUPPLY, FACTORY SETUPS, SITE PREP.

EARLY **2030s**
US SMR ASSEMBLY, TESTING, COMMISSIONING; FIRST FLEETS SUPPORT MAJOR DATA CENTERS.

Potential Resource Challenges for US Energy

FUEL SUPPLY CONSTRAINTS AND DELAYS

A critical requirement for these nuclear deployments is the availability of HALEU–enriched uranium with a U-235 concentration between 5 and 20 percent. This specialized nuclear fuel makes advanced SMRs and generation IV reactors more compact, efficient, and economically viable. China's well-established HALEU production infrastructure provides it with a strategic advantage in fueling SMRs at scale with less dependence on imports, accelerating its SMR rollout.

The US is still building commercial-scale HALEU (e.g., Centrus Ohio, DOE HALEU Availability Program), but regulatory, supply chain, and capital constraints risk pushing deployment to the early 2030s.

A NEW FRONT IN US-CHINA COMPETITION

The US faces structural challenges in scaling its energy infrastructure to meet AI data center demand. A decentralized, privatized energy sector, combined with stringent regulatory and market dynamics, slows grid upgrades and renewable integration. These bottlenecks threaten hyperscale providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) – the backbone of US AI capabilities – and risk undermining national competitiveness while reducing strategic flexibility. SMRs remain a pathway to stable, carbon-free power, but only if licensing, HALEU supply, and investment hurdles are resolved quickly.

The nuclear energy dimension deepens the geopolitical competition between China and the US. SMRs and advanced generation IV reactors will become strategically important factors alongside renewables, critical minerals, and digital infrastructure.

China's state-driven SMR deployment, paired with renewables, accelerates its energy security, climate goals, and geopolitical leverage. The US must accelerate nuclear innovation and deployment or risk ceding both commercial advantage and strategic influence. The intensification of nuclear-related technology, regulatory, and supply chain competition will likely escalate bilateral economic tensions.

OUTLOOK

The integration of nuclear energy into AI's power-supply architecture will be decisive for US-China competition and global technology leadership. China's early SMR deployment lead, paired with renewables, advances both climate and geopolitical goals. The US faces a pivotal window in which to accelerate SMR deployment and domestic HALEU production to sustain AI infrastructure growth and its technological edge.

As AI-nuclear interdependence deepens, expect geopolitical risk to rise, requiring careful oversight to manage rivalry while preserving global economic stability.

SIGNALS TO WATCH

- → Growth in state-sponsored cyber or physical probes targeting nuclear/HALEU supply chains.
- → Introduction of new US or Chinese nuclear licensing frameworks or fast-tracked approvals.
- → Market shifts in uranium/HALEU pricing and supply contracts.

Nuclear power station.

AMERICAS

EXECUTIVE SUMMARY

In 2026, businesses across the Americas will face heightened security risk driven by evolving criminal tactics, major event disruptions, and grievance-driven violence. Latin American organized crime groups will increasingly use drones, AI, and smuggling innovations, expanding beyond drug trafficking into illegal mining and cybercrime; these shifts will strain corporate security and supply chains. The FIFA World Cup will create operational and reputational challenges through heightened security, protests, and exploitation by Mexican drug-trafficking organizations (DTOs). In the US, targeted violence by lone actors will rise, threatening prominent corporate leaders, political figures, industries, and infrastructure.

EVENTS TO WATCH

- **World Cup security/protest flashpoints:** As security perimeters tighten and activist networks target games and transport nodes, expect road closures, delivery and visa delays, and brand risk for sponsors/near-venue businesses.
- **Remote/automated scale-up of trafficking:** As drug trafficking organizations expand and innovate, expect higher interdiction evasion, maritime insurance/cargo-screening pressure, and import/export exposure from disguised mercury shipments.
- **US grievance-driven targeting:** Polarizing triggers (policy fights, high-profile incidents, and the midterm elections) will increase lone-actor threats against executives, media/political organizations, and tech infrastructure.

KEY JUDGMENTS

Organized crime groups in Latin America will weaponize drones, AI, and new smuggling methods to diversify beyond drug trafficking, escalating risks to corporate security, cyber resilience, and supply chains.

Heightened security, protests, and DTO exploitation will create significant operational and reputational risks for businesses near FIFA World Cup venues in the US, Canada, and Mexico.

In the US, lone actors driven by grievances and polarization will increasingly target corporate and political leaders, industries, and infrastructure, amplifying threats to personnel and assets. Large public gatherings will be particularly vulnerable to mass casualty events.

Aerial view of New York City streets at night.

Latin American Organized Crime Groups' Use of Technology to Increasingly Threaten Business Operations

Organized crime in Latin America is entering a new technological phase driven by the use of drones, AI, and innovations in smuggling technologies, allowing groups to diversify their criminal activities. These changes will affect corporate security in 2026. For companies operating in or tied to the region, this shift broadens risks across physical security, cyber resilience, and supply chain integrity.

EXPANDING CRIMINAL USE OF DRONES AND AI

Latin American organized crime groups will increasingly leverage drone technology in 2026 to threaten government forces, extort businesses, and fight rival groups. Mexican DTOs are at the forefront; the Jalisco New Generation Cartel (Cártel de Jalisco Nueva Generación, CJNG), for instance, maintains a dedicated branch of drone operators. As the CJNG and other Mexican DTOs expand their influence across the region, criminal drone use will likely spread to other countries – posing serious challenges to corporations that struggle to mitigate threats by criminals who use drones for surveillance and kinetic action.

Colombia: Major armed groups have already been aggressively acquiring commercial drones and will likely use them to surveil kidnapping targets and signal threats to businesses that resist extortion demands; even a simple overflight of a commercial site can demonstrate vulnerability and prompt payment. Such groups have also already demonstrated the lethal potential of drones. In August 2025, a dissident faction of the Revolutionary Armed Forces of Colombia (Fuerzas Armadas Revolucionarias de Colombia, FARC) flew a drone packed with explosives into a police helicopter during a coca-eradication operation, killing 12 officers – one of the group's most successful attacks in recent years. The FARC, as well as the National Liberation Army (Ejército de Liberación Nacional, ELN) and the Gaitanista Army of Colombia (Ejército Gaitanista de Colombia, EGC), will likely attempt similar operations in 2026, either by flying explosive drones into targets or by rigging mortar rounds to quadcopters to drop on rival positions.

Brazil: The Red Command (Comando Vermelho, CV) and the Third Pure Command (Terceiro Comando Puro, TCP) will increasingly rely on drones to monitor areas dominated by rival groups, especially in Rio de Janeiro, where incidents of traffickers using drones to drop explosives in areas dominated by rivals have already occurred. Drones are also being increasingly used to monitor and coordinate drug-trafficking operations, including via São Paulo's Guarulhos International Airport, and to track police activity, complicating operations against organized crime. Operational risk assessments will be critical to navigating urban areas in Brazil, particularly in Rio de Janeiro. They should account for protocols allowing local operators to pause, reroute, or relocate operations when drone activity is confirmed over company sites or lanes.

In addition to increased use of drones, AI adoption by criminal groups will likely accelerate in 2026. Virtual kidnapping, in which targets are deceived into believing a loved one or business associate has been abducted, will be facilitated by AI voice synthesis, increasing both the efficiency and profitability of such operations. Criminal networks will also use AI voice synthesis in social engineering attacks that attempt to convince company employees that management has authorized transfers of money or password resets. In Brazil, criminals will increasingly use AI-generated voice technology to run scams related to the Central Bank's PIX payment system. Beyond voice imitation, AI-generated deepfake images and videos can be deployed for sextortion and propaganda purposes. Colombia's EGC, for example, has started using deepfake videos featuring fictitious news anchors reporting on the group's purported victories.

AI-facilitated cybercrime will continue to be a growing problem in the region. Tools intended to help ethical hackers find and patch vulnerabilities in web systems will increasingly be repurposed by criminal groups to exploit those weaknesses first. AI will also help relatively unsophisticated criminal actors code ransomware targeting critical infrastructure (such as ports and pipelines), forcing companies to pay – usually in cryptocurrency – to resume critical operations.

TECHNOLOGICAL INNOVATION IN SMUGGLING AND NONTRADITIONAL MARKETS

Organized crime groups will further rely on technological innovation to smuggle contraband across borders. In July 2025, the Colombian Navy seized an unmanned semisubmersible outfitted with a Starlink antenna in the Caribbean. Though empty at capture, the craft was almost certainly being remotely steered by a DTO testing it for future use to traffic cocaine across the Caribbean for end-use in the US. While the craft was seized, its existence demonstrates a desire by DTOs to use technology to avoid arrests at sea. Recent moves by the US Navy to deploy lethal force against drug trafficking vessels will only increase incentives to further develop such technologies.

Latin American criminal groups will also likely increasingly depend on technology to expand their influence over black and grey markets beyond traditional drug trafficking. With gold prices at historic highs, major criminal organizations will deepen ties to illegal gold mining and use new methods to smuggle mining chemicals and gold – even marketing their technological know-how to illegal miners. Mexico's CJNG has a head start in the race to provide such services; it has strong ties to mercury mines in Querétaro State and is developing systems to infiltrate mercury into otherwise legitimate shipments so illegal gold miners can intercept it, as the chemical is used to separate gold from ore. CJNG will probably market these services to criminal organizations such as the ELN, which illegally mines gold in Venezuela, and several smaller organizations in Peru and Ecuador that run similar illegal mining operations.

One early yet illustrative foray of Mexican DTOs into illegal gold mining in South America may have been exposed in July 2025, when authorities at the Port of Callao in Peru discovered that a shipment of Mexican gravel destined for Bolivia had been impregnated with approximately four metric tons (4.4 short tons) of mercury. The shipment of mercury, a toxic chemical that causes extreme health risks in areas where illegal mining occurs, appears to have represented an effort by the CJNG to expand its operations in South America. Because the CJNG and other Mexican DTOs are so violent, any increase in their activities outside of Mexico would bode poorly for security in the affected countries, and the infiltration of a toxic substance into international shipments will be a growing concern for importers and exporters in 2026.

Taken together, these examples underscore a broader trend: Latin American organized crime groups are no longer solely reliant on drug smuggling, instead diversifying their criminal portfolios and modernizing through rapid technological adoption. For businesses, the 2026 threat environment will be shaped by drones, AI-enabled scams, cyber intrusions, and physical violence. Proactive operational risk assessments and planning will be critical to safeguard operations, assets, and personnel in Latin America.

Illegal drone carrying a package filled with narcotics.

FIFA World Cup to Cause Significant Disruptions Across the US, Canada, and Mexico

The 2026 FIFA World Cup will create significant operational and reputational challenges for businesses near event venues, driven by heightened security measures, potential political protests, and large-scale crowd management. Venue security will likely disrupt commercial activity via road closures, area access restrictions, and intensified screening protocols. Politically charged demonstrations may target the event, generating reputational risk for companies associated with the World Cup and causing additional operational interruptions. Businesses that anticipate these challenges – and implement proactive strategies to manage crowd-related disruptions, navigate politically sensitive situations, and maintain operational continuity – will be better positioned to safeguard assets and capitalize on opportunities presented by the event.

BUSINESSES THAT ANTICIPATE CHALLENGES ASSOCIATED WITH THE WORLD CUP WILL BE **BETTER POSITIONED TO** SAFEGUARD ASSETS AND **CAPITALIZE ON OPPORTUNITIES** PRESENTED BY THE EVENT.

TARGETS OF OPPORTUNITY FOR CRIME AND ACTIVISM

Venue security will likely require extensive coordination and could disrupt surrounding commercial activity. The 2024 Copa América final in Miami, where crowds overran security barriers and forced a delay of the game, will prompt World Cup organizers to adopt more proactive, layered security measures. These may include expanded perimeters, road closures, and more intensive screening protocols, with people who do not have tickets probably barred from even approaching some stadiums. Businesses near the games – including retail and hospitality services – may experience altered customer flow, temporary closures, or operational delays; transportation-dependent companies will need contingency plans for rerouted traffic and delivery schedules. For travel to the host nations – particularly the US – the demand for visas will surge to the point where business travelers and relocating workers may face prolonged waits in obtaining necessary travel documents.

Criminal organizations will likely attempt to turn the increased economic activity that accompanies the World Cup to their advantage. In Mexico, DTOs will seek to set up front companies to win vendor contracts, posing legal risk to companies that inadvertently engage them – especially now that Mexico's main DTOs have been designated as foreign terrorist organizations by the US government. DTOs will also likely seek to profit from the World Cup in other ways, such as selling counterfeit tickets to games, setting up illegal gambling rackets, and running prostitution rings.

Even in the absence of a direct security incident, the World Cup may create reputational and operational risks for businesses sponsoring or otherwise associated with the event. Heightened political tensions surrounding immigration enforcement and US domestic policy could expose companies to public scrutiny. The presence of Immigration and Customs Enforcement (ICE) agents, as rumored based on prior events like the FIFA 2025 Club World Cup, will lead to tensions with protesters, creating uncertainty for businesses located near venues. Firms may need to develop communications strategies and operational adjustments to mitigate the risk of disruption from politically charged incidents.

Activist groups will almost certainly seek to take advantage of the World Cup as a high-visibility platform to draw greater attention to their causes. These will likely include groups concerned with the conflicts in the Middle East, particularly in Canada and the US, as well as those critical of US President Donald Trump's administration and its immigration policies. Pro-Palestinian activists have previously forced the cancellation of smaller-scale sporting events in Europe, such as the Vuelta a España; in 2026, such groups will likely attempt to achieve a similar outcome at a larger-scale event like the World Cup. Protestors may seek to interrupt games or associated events or enact blockades close to FIFA events, prompting significant traffic congestion and disruptions to commercial activity at World Cup venues. Scuffles are possible if authorities opt to forcibly remove activists who refuse to disperse from key transit routes near key venues.

Overall, the 2026 FIFA World Cup presents significant opportunities for businesses but also introduces complex operational and reputational risks. Companies that proactively anticipate border delays, heightened security, and protest-related disruptions will be better positioned to maintain continuity, safeguard employees and assets, and capitalize on commercial opportunities associated with this global event.

SoFi Stadium in Inglewood, California, to host FIFA World Cup 2026 games.

Targeted Violence Likely to Increase in the US

PERSONAL GRIEVANCES LIKELY TO MOTIVATE ATTACKS

The US will likely continue to see an increase in targeted attacks by individuals who blame specific companies or people for their problems, as well as political extremists. Likely targets include political and media figures, as well as individuals who work within certain industries – particularly finance, healthcare, and technology. Attacks may occur in a variety of settings, from offices to public events and even the homes of victims; perpetrators will seek to carry out high-visibility actions to draw attention to perceived injustices.

Targeted violence is likely against organizations the perpetrators believe harmed their personal health or wealth, a form of violence related to but distinct from mass shootings in which the public is targeted nearly at random. Such incidents have already occurred with the killing of a health insurance executive in late 2024, as well as attacks against the National Football League (NFL) and the US Centers for Disease Control and Prevention (CDC) in 2025. In all these cases, the perpetrators appear to have been motivated by the belief that the organization had directly harmed their personal health or well-being.

Copycat incidents will likely occur in 2026, particularly among disturbed individuals facing severe health or financial stress. Potential targets include healthcare providers, hospitals, and pharmaceutical firms; financial institutions such as banks, real estate firms, and private equity companies may also face heightened risk, especially if the US experiences economic headwinds. Technology companies and their executives remain vulnerable as well, given perceptions of growing influence, social disruption, and intrusion into everyday life. Conspiracy narratives surrounding the sector may amplify threats. Companies engaged in politically visible or government-linked activities will also face an elevated risk of being affected by such violence.

THE IMPACT OF A POLARIZED SOCIETY

Political polarization will also remain a powerful motivator. Lone actors radicalized by ideological narratives will view opponents not just as adversaries, but as morally wrong, dangerous actors responsible for ongoing societal harm. As a result, politicians, media commentators, and politically active organizations will be likely targets in 2026.

The political, social, and economic repercussions of the US government shutdown will be felt well into 2026. Rhetoric and political activism will ramp up by the summer for the midterms, and it is likely that political narratives will be amplified during the World Cup – particularly those on income inequality, crime, and immigration. Polarizing political rhetoric will be high during the 2026 election cycle, but widespread violence is unlikely. Major events like the World Cup often represent targets and stages of opportunity for violent extremists and radicalized individuals, but such attacks will remain isolated in nature.

These lone-actor attacks may take a variety of forms. Individuals may carry out attacks on corporate offices, large events such as conferences or gatherings, or individual business leaders, including when they are at home or commuting. Attackers will likely concentrate efforts on actions with a highly visible profile, making violent assaults on individuals more desirable for some attackers than destructive actions carried out against property.

Nonetheless, property associated with the tech industry (data centers, communications hardware, or products) may also be damaged or destroyed due to their symbolic value. Mass arson at Tesla dealerships in 2025 by those opposed to CEO Elon Musk's activities with the US Government exemplifies the potential for high-visibility, destructive acts against tech infrastructure. The example raises the possibility that individuals may carry out destructive acts that are less immediately harmful to human life but are likely to occur more frequently, precisely because the actions are seen as less serious and easier to commit. Consequently, attacks on property and infrastructure – particularly in tech – are likely to rise.

Overall, the rising threat environment is shaped by individuals who perceive themselves as harmed or marginalized by powerful institutions. A growing number of such actors are likely to translate personal grievances into violent and destructive action, targeting both people and assets associated with political or corporate authority.

US Capitol building in Washington, DC.

ENVIRONMENT

SEVERE WEATHER LIKELY TO IMPACT THE 2026 FIFA WORLD CUP

EXECUTIVE SUMMARY

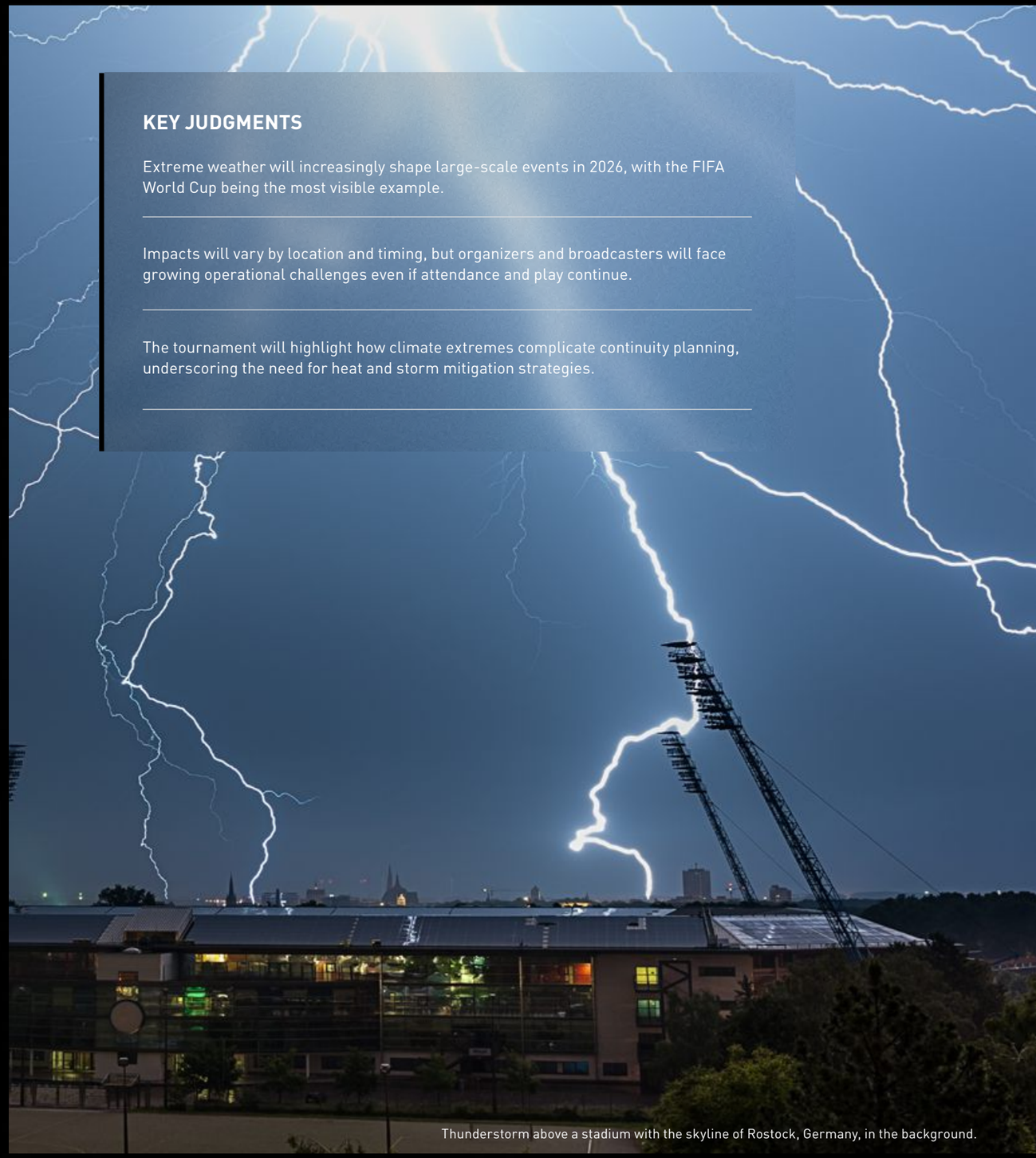
Extreme weather will have an increased influence on large-scale, global events in the coming year, with heat and severe thunderstorms likely to impact the 2026 FIFA World Cup in North America. Conditions are unlikely to stop fans from attending or players from competing, but they could diminish the experience for participants and spectators, and pose serious challenges for tournament organizers and broadcasters. The World Cup will likely illustrate how flagship events are increasingly shaped by severe weather, highlighting the need to anticipate heat and storm risk while maintaining event continuity.

KEY JUDGMENTS

Extreme weather will increasingly shape large-scale events in 2026, with the FIFA World Cup being the most visible example.

Impacts will vary by location and timing, but organizers and broadcasters will face growing operational challenges even if attendance and play continue.

The tournament will highlight how climate extremes complicate continuity planning, underscoring the need for heat and storm mitigation strategies.



Thunderstorm above a stadium with the skyline of Rostock, Germany, in the background.

Threat Landscape

EXTREME HEAT

Extreme heat is expected to be a major issue for both players and attendees during the tournament. Between June 11 and July 19, 2025 – the same window when the tournament will take place – 13 of the 16 host cities recorded temperatures above 30 C (86 F). Vancouver narrowly missed the threshold at 29.9 C (85.8 F). Several locations experienced peaks near 38 C (100 F), with heat persisting for multiple days.

Global temperatures continue to rise, and next year's tournament will likely experience similar temperatures. These factors will not stop matches or fans, but they will intensify operational burdens, stress infrastructure, and elevate health risks for athletes, spectators, and staff.

STORM AND HURRICANE RISKS

Warmer temperatures also contribute to more intense thunderstorms, as greater heat drives evaporation and allows clouds to hold more moisture. Lightning protocols are clear: in the US, play is suspended for 30 minutes if a strike is detected within roughly 10 km (6 miles) of a stadium, and fans are directed to shelter. Each additional strike resets the 30-minute clock. Similar rules are in place for Canada and Mexico.

The Atlantic Hurricane season starts in June. While major storm systems are less common early in the season, there is still a potential that storms could develop and impact venues including Miami and Houston on the Gulf Coast, and possibly further inland locations like Monterrey, Dallas, and Atlanta. Hurricanes or strong tropical storms could force game cancellations in affected cities and disrupt domestic travel.

CASCADING IMPACTS

In extreme cases, heat and severe storms pose direct health threats to players and attendees. Increased wildfire activity due to extreme temperatures can have additional impacts on health due to poor air quality, and can also disrupt transport, particularly in more remote areas. Severe weather also reduces athletic performance, undermines the spectator experience, and creates costly complications for broadcasters and tournament organizers. Delays may force networks to shift airtime, lose advertising slots, or renegotiate compensation, while persistent disruptions could erode future rights fees. Organizers face increased operating costs from extended staffing during delays, and – if a match is cancelled or abandoned – the difficult task of rescheduling within an already packed schedule.

INFRASTRUCTURE AND SCHEDULING CONSTRAINTS

Only four of the 16 stadiums set to host matches (Atlanta, Dallas, Houston, and Vancouver) have retractable roofs and climate-controlled stadiums that can mitigate the impacts of severe weather. Even with this infrastructure, forecasts suggest Dallas and Houston could reach dangerous temperatures during afternoon games.

Match kick-off times will not be confirmed until after December's draw. Shifting games to earlier in the day or later in the evening could help avoid peak heat, but would risk clashing with FIFA's priority to maximize viewership in key European markets. A central challenge will be whether organizers can allocate afternoon matches to more climate-controlled stadiums or cooler host cities once the schedule is finalized.

Threats and Cascading Impacts at the 2026 FIFA World Cup

PRIMARY THREAT	DIRECT IMPACTS	CASCADING IMPACTS
EXTREME HEAT	High temperatures (30-38 C), prolonged heatwaves	Player fatigue and reduced performance; heat illness among fans; strain on medical response; infrastructure strain, health and disruptive impacts of wildfires
SEVERE THUNDERSTORMS	Lightning delays; heavy rainfall; power and transport disruptions	Match suspension; crowd safety challenges; extended staffing needs; degraded spectator experience
HURRICANES / TROPICAL STORMS	Venue damage risk; flooding; travel disruptions across Gulf and inland cities	Possible game cancellations; large-scale rescheduling; mass transit strain; stranded fans and staff
COMBINED EFFECTS (HEAT + STORMS)	Concurrent stress on health, safety, and logistics	Increased broadcaster costs (airtime shifts, lost ad slots, reduced rights value); higher organizer costs (staffing, contingency ops); reputational impact on event delivery

2026 FIFA World Cup Host Cities

Issues Highlighted During the 2025 World Cup

EARLY WARNING SIGNS FOR 2026

The 2025 FIFA Club World Cup, held in June-July, was seen as a test event for the 2026 tournament. Although hosted solely in the US and with just five overlapping venues, it revealed challenges that are likely to recur. Excessive heat affected much of the eastern US, forcing water breaks during matches, limiting outdoor training, and reducing player intensity on the field.

Severe weather also caused repeated disruptions. Six of the 63 matches were stopped for lightning, with delays ranging from 46 minutes to nearly two hours. Teams faced additional travel complications due to storms.

The 2026 World Cup will be larger in every respect – 48 teams instead of 32, 104 matches instead of 63, and higher attendance. With little flexibility for delays or rescheduling, and with a global audience watching, the ability of organizers to respond effectively to weather challenges will be under close scrutiny.

OUTLOOK

Weather disruptions at the 2026 FIFA World Cup are virtually certain, even if their scale varies from venue to venue. The tournament will test how well organizers can balance player safety, fan experience, and broadcasting commitments against extreme heat and storm risks. Impacts may range from minor inconveniences to serious health concerns, underscoring the need for both organizers and attendees to plan for mitigation measures.

Stronger Responses Required

Organizers and local authorities will need to strengthen contingency planning to manage the combined risks of extreme heat, severe storms, and hurricanes. While stadium infrastructure and established lightning protocols provide a degree of protection, the scale of the 2026 World Cup will stretch medical services, transport systems, and broadcasting schedules. Effective risk management will depend on both long-term planning and real-time flexibility.

MITIGATION STRATEGIES

- **Heat Management:** Provide cooling zones and hydration stations, and enforce scheduled water breaks to reduce health risks for players and fans.
- **Storm Protocols:** Apply lightning delay rules consistently across venues, and ensure clear communication channels for spectators and staff.
- **Resilience Planning:** Pre-establish contingency windows, rescheduling options, and broadcaster coordination to manage prolonged or repeated delays.
- **Medical and Staffing Support:** Increase on-site medical presence, and extend staffing flexibility to handle disruptions and emergency responses.

SIGNALS TO WATCH

- **Kick-off Scheduling:** Match times announced in December will show how organizers balance heat risks against European broadcast priorities.
- **Stadium Allocations:** Placement of afternoon games in climate-controlled or cooler venues will reveal FIFA's willingness to adapt scheduling.
- **Storm Season Severity:** Early hurricanes or unusually frequent thunderstorms could foreshadow major disruptions in southern and Gulf Coast cities.

RECOMMENDED ACTIONS

Program-Level Actions

- Expand heat and storm contingency plans to cover all 16 host cities, accounting for differences in infrastructure and climate exposure.
- Develop rescheduling protocols in advance, including contingency windows and communication frameworks.
- Establish clear coordination between FIFA, local emergency services, and broadcasters to ensure consistent responses to delays or cancellations.
- Allocate additional resources for medical staffing, hydration facilities, and cooling zones.

Day-to-Day Measures

- Monitor local forecasts continuously, with dedicated staff assigned to stadium weather tracking.
- Adjust training schedules and transportation plans in response to daily conditions.
- Enforce lightning and heat protocols consistently, including mandatory water breaks and temporary evacuations when thresholds are met.
- Communicate proactively with fans about safety procedures, shelter options, and schedule changes.

EUROPE

EXECUTIVE SUMMARY

US and European divisions over the enduring Russia-Ukraine conflict will likely deepen in 2026, with Washington favoring secondary measures and episodic diplomacy while Europe advances rolling sanctions. The broadening divide will deepen compliance gaps, presenting risks and opportunities for foreign businesses seeking to operate in Russia, where the risks of legal complexity, detention, and corruption remain. Countries on the EU's eastern flank will grapple with Russian influence, pressure on populist leaders, and volatile elections - notably in Hungary - sustaining civil unrest, instability, and operational uncertainty for businesses across this region. Some countries will also face sustained online misinformation campaigns and an elevated threat of cyber-attacks aiming to disrupt public services and undermine democratic institutions.

EVENTS TO WATCH

- **Hungary's April 2026 election:** Continued curbs on assembly combined with a likely spike in Russian or pro-Russia online influence campaigns will exacerbate mass protests, strike risk, and travel/security constraints in Budapest and other hubs.
- **EU sanctions cadence vs. liquified natural gas (LNG) cutoff by end-2026:** Budapest and Bratislava's continued effort to dilute packages or slow implementation will contribute to widening EU-US gaps, higher compliance complexity, and counterparties exploiting loopholes.
- **US-Russia diplomatic spurts (prisoner swaps/asset overtures):** The perceived thaw in the US-Russia relationship will prompt some firms to test re-entry or recovery; sudden reversals would raise detention and asset-seizure exposure.

KEY JUDGMENTS

EU Russia policy will fragment, driving policy uncertainty and uneven compliance regimes, which will present business planning risk.

Operating in Russia remains high-risk amid legal obstacles, asset controls, corruption, and detention exposure – making exits or returns costly.

Asset-recovery and re-entry signals will surface, but clashing US/EU/G7 regimes and reputational blowback will deter moves.

Hungary, Serbia, and Georgia remain polarized; Romania and Moldova consolidate pro-EU control – sustaining protest and policy volatility.

Sofiyivska Square - Kyiv, Ukraine.

Europe-US Divisions Over Russia-Ukraine Conflict Likely to Worsen in 2026

DIFFERING OBJECTIVES

The US and European visions of how to end the conflict will likely remain far apart through 2026. Washington remains open to Ukrainian territorial concessions in exchange for peace and is unlikely to impose sweeping sanctions on Russia. European leaders reject land swaps outright and will continue to punish Moscow through sanctions, particularly amid escalating aerial strikes in Ukraine and increasing security tensions between Russia and Eastern European nations.

High-level diplomacy will ultimately conclude the Russia-Ukraine conflict, but both sides, for now, remain determined to fight; over the short term, further direct diplomacy between Trump and Putin without any conditions, which European leaders strongly oppose, is unlikely to resolve the conflict. Unwilling to press Moscow itself or carry the financial burden of brokering peace, Washington will likely maintain pressure on Europe to cut all trade ties with Russia and to increasingly take the lead in financially and materially supporting Ukraine's defense. While the US is hesitant to impose new sanctions on Russia despite bipartisan congressional appetite to act, Washington has imposed secondary sanctions and tariffs on nations doing business with Moscow, including India. Notably, additional tariffs have not been imposed on China, the largest purchaser of Russian hydrocarbons, or fellow NATO nations Hungary and Slovakia, which each receive over 80 percent of their oil from Russia.

Rather than targeting Hungary or Slovakia directly, which would be challenging given that their trade is conducted under the EU's banner, the US has used their relationship with Russia to highlight EU inconsistency. Additional US measures on Russia are now likely to hinge on Europe imposing a full trade embargo. Under US pressure, the EU has pulled forward its Russian liquified natural gas (LNG) ban from 2027 to the end of 2026, but Washington has not signaled parallel action once that ban comes into effect. Such parallel action is improbable if Moscow continues episodic diplomacy, prisoner exchanges, or limited de-escalation.

Policy distance will almost certainly persist between Washington and European capitals, particularly amid selective US diplomatic engagement and use of secondary sanctions tools in opposition to the EU- and G7-led sanctions cadence. Growing ambivalence towards sanctions will weaken collective leverage over Moscow. Additionally, the resulting policy and legal uncertainty will sustain planning and compliance ambiguity for businesses.

DIVERGING SANCTION POLICIES

European governments – pressed to lead Ukraine's defense – will, through 2026, impose regular tranches of sanctions on Russia, targeting the defense and finance sectors, the shadow fleet, and third-country evasion networks. However, with governments in Hungary and Slovakia prioritizing national interests over Ukraine's defense and broader European security concerns, the EU will likely find it increasingly difficult to impose the harshest sanctions. Budapest and Bratislava may also point to continued diplomacy between the US and Russia as signs that some level of relationship can be maintained.

The deepening wedge between Brussels and Washington in finding a common stance on Russia will likely result in an uncoordinated sanctions regime and competing long-term policies. While the US has not relaxed any sanctions on Russia, it failed to join its European allies in any of the regular sanction packages announced in 2025. This leaves significant gaps in the enforcement regime, despite increased European efforts to penalize Russia's economy. Additionally, continued US diplomatic engagement with Moscow, though unlikely to end the conflict or the global sanctions regime in the medium term, has signaled a potential end to Russia's economic isolation.

Some Western firms – especially those whose stakes were seized by Moscow – will increasingly seek recovery or limited re-entry in 2026. The August 2025 Alaska summit coincided with a Russian presidential decree enabling ExxonMobil to recover its multi-billion-dollar stake in the Sakhalin-1 oil and gas project. Subsequent talks with Rosneft suggest selective economic relief rather than a return to operating in Russia. Nonetheless, the decree indicates an opportunity for Russia and the US to repair their commercial relations, a development that – while potentially positive – would expose businesses to a host of return-related challenges.

Multiple sectors of the Russian economy will remain under sanctions through 2026. In the unlikely event that the US lifts some sanctions to allow for the return of a select group of major US businesses, those companies would still face operating in violation of EU, UK, and G7 sanctions, as well as reputational harm and Russian countersanctions. In this environment, companies based in countries not closely aligned with Western nations will likely seek to capitalize on the thawing of US-Russia relations and the increasingly uncoordinated sanctions regime.

Snow-covered anti-tank obstacle used by military.

CHALLENGES TO OPERATING IN RUSSIA

Foreign businesses face a hostile legal environment and high corruption risk. Russian business and political elites maintain relationships based on nepotism, clientelism, kickbacks, and bribery. Business leaders leverage these relationships to ensure that foreign assets remain under domestic control. Authorities can block sales of seized assets and terminate buyback clauses on vague grounds, while Russian companies lobby for harsh terms governing the return of any foreign business.

Foreign nationals – especially from NATO countries – will continue to face an elevated potential for arrest and detention by government authorities over the foreseeable future. Until relations between Moscow and the West normalize, Russia will be motivated to use the judiciary to pressure adversaries. Foreigners are vulnerable to harsh applications of local laws and increased scrutiny by officials. Detainees are often treated as bargaining chips in exchange for Russian nationals detained in the West.

Any further formal or informal rapprochement between Washington and Moscow would likely signal an opening to foreign businesses. However, foreign companies will need to monitor several indicators, including legislative initiatives in Moscow, the return of seized assets, and the US approach to Ukraine and the EU, which could either facilitate or complicate business resumption. Diplomatic engagement is primarily driven by the Trump-Putin relationship, rather than geostrategic developments. Accordingly, any rapprochement could swiftly sour in response to minor incidents. This could pose a significant risk to personnel operating in Russia, who may find themselves at an increased risk of detention.

Diplomatic engagement is primarily driven by the Trump-Putin relationship.

Authoritarianism and Counter-Movements on the EU Periphery

Civil unrest and political instability will likely increase on the EU's periphery through 2026. Eastern European countries sit on the political front-line between Moscow-backed authoritarianism and the EU's bureaucratic democracy. The Ukraine conflict, energy security, and EU accession debates will drive regional geopolitics and keep domestic politics taut. Anti-government protests over weak economic growth and corruption will continue to spread, and rising Russian interference, mis- and disinformation campaigns, and disruptive cyberactivity will continue to sustain instability.

Perceived failings by some populist leaders are boosting support for pro-EU groups. Anti-EU leaders in Georgia, Hungary, and Serbia continue to face sustained campaigns against corruption and maladministration. Meanwhile, pro-EU governments in Moldova and Romania have survived despite intense Russian pressure, sustained misinformation campaigns, and attempts to undermine democratic institutions. In Slovakia, Prime Minister Robert Fico, who consistently opposes greater multinational action against Russia, appears increasingly isolated.

Hungary will hold general elections in April 2026; Prime Minister Viktor Orban could lose power after 15 years of increasingly authoritarian rule. Even with a shift towards Brussels, reversing a long illiberal period will take time, and regional geopolitics will remain taut while the Russia-Ukraine conflict persists.

HUNGARY

Prime Minister Viktor Orban has dominated Hungarian politics for nearly 30 years but could lose his grip in April 2026. He has increasingly embodied conservative populism – politicizing state media and the judiciary, disrupting EU cohesion, and echoing some anti-Western narratives that often emanate from Moscow. Russia's 2022 invasion of Ukraine exacerbated the tensions between Budapest and Brussels, as Orban has delayed or vetoed EU sanctions and NATO support to Kyiv. However, domestic pressures, including a lagging economy and entrenched corruption, will likely define the election.

Two rival movements gained traction in 2025. Peter Magyar split from Orban's Fidesz party to found Tisza (Respect and Freedom). A traditional conservative, Magyar will likely continue campaigning against corruption and scandals around senior figures close to Orban, and he will almost certainly be the main contender to challenge the Prime Minister during and after the April elections. Separately, a progressive movement swelled after Budapest initially banned the 2025 Pride festival; rallies have drawn tens of thousands demanding freedom of assembly. Similar mobilizations are highly likely through early 2026 and could escalate if authorities restrict the campaign. It is highly likely that the Hungarian cyberspace and online discourse will see an increase in misleading and disingenuous narratives driven by pro-Russia or anti-opposition figures; this could skew the electoral narrative and inflame political tensions.

European authorities will likely watch closely for any attempt by Moscow to covertly influence the April election through social media campaigns, the promotion or undermining of political figures, and stoking nationalist civil unrest. In the event of another Orban victory, opposition politicians and campaigners will likely launch widespread protests. If Orban is ousted, the country will still face an extended period of economic and domestic political tension.

SLOVAKIA

Prime Minister Robert Fico faces growing international isolation and domestic pressure. Opposition-led mass rallies will likely continue through 2026, ahead of general elections scheduled for 2027; however, opposition leaders will likely continue to press for early elections.

Fico draws criticism for his closeness to Putin and for deepening the country's reliance on Russian energy imports. He was the only EU/NATO leader to attend the 2025 Shanghai Cooperation Organization summit in China, and even his political allies have criticized his remarks about Ukrainian leader Volodymyr Zelenskyy. In 2026, Fico is unlikely to back down from his anti-EU stance; he will pursue more authoritarian or isolationist policies despite his Smer-SD trailing the Progressive Slovakia party in the polls. Such policies would likely prompt further domestic polarization and anti-government civil unrest.

SERBIA

Mass anti-government protests by pro-EU opposition parties will likely destabilize Serbia through 2026. Demonstrators are pressing for early elections and President Aleksandar Vucic's resignation; student and civil-society groups have staged near-daily rallies in Belgrade and other cities. The government has stood firm; violence between protesters and police or pro-government actors is common, and arrests of activists have further escalated tensions.

Russian authorities have intervened, repeatedly claiming that the protest movement is a Western-orchestrated attempt at regime change; however, Belgrade will likely maintain its policy of balancing the EU and Russia. With neither side willing to back down and elections not scheduled until 2027, instability in Serbia will likely increase.

GEORGIA

Georgia's relatively EU-skeptic government will continue consolidating control while containing a long-running opposition movement – making large-scale protests unlikely to destabilize the country. The ruling Georgian Dream party has consistently pursued policies that undermine the country's EU accession and implemented increasingly illiberal policies. A nationwide anti-government protest movement continued through 2025, denouncing the party's perceived anti-EU policies. However, authorities appear to have largely pacified the protests, leaving anti-government activists lacking the institutional and popular leverage to challenge the country's drift from the EU.

Unlike with Serbia, the EU has taken an active role in Georgia's political tensions by denouncing Tbilisi and sanctioning senior government figures for alleged corruption and human rights violations; additional sanctions are almost certain through 2026. Coupled with the erosion of anti-corruption institutions, these steps will deepen challenges to foreign businesses operating in Georgia.

ROMANIA

Romania's centrist, pro-EU government will likely act as a stabilizing influence in the region through 2026, following a turbulent, polarizing period. In May 2025, Nicusor Dan won the presidency on an anti-corruption platform, defeating first-round leader George Simion, an EU-skeptic populist. The contest followed a November 2024 presidential poll won by pro-Russia candidate Calin Georgescu. Romania's constitutional court overturned the result, citing evidence of Russian-backed interference, including a sustained misinformation campaign conducted by bots and paid influencers via social media.

The Romanian government will continue to face economic, domestic, and Ukraine conflict-related pressures; however, Bucharest will likely avoid the mass protest campaigns likely in neighboring countries through 2026, though the extreme election interference episode serves as a warning to regional capitals about vulnerability to foreign influence. Despite previously overcoming these challenges, Romania will continue to be a target of online misinformation campaigns driven by pro-Russia groups and cyberattacks attempting to disrupt public services and logistics.

MOLDOVA

Pro-EU forces will likely consolidate institutional control through 2026 despite sustained Russian influence campaigns. Voters have repeatedly backed liberal, pro-EU parties, and in 2025, judicial authorities banned the pro-Russian Heart of Moldova and Moldova Mare parties for alleged Moscow-backed misconduct. In 2026, authorities will likely seek to ban additional pro-Russian groups, including Chance and Revival, almost certainly drawing outrage from Moscow and prompting renewed destabilization efforts.

Russia will likely intensify pressure via disinformation, support for anti-government protest groups, and efforts to stoke sentiment in Gagauzia, an autonomous region of the country with elevated levels of pro-Russian sentiment. Moscow may also exacerbate political tensions between Chisinau and the Russia-friendly separatist region of Transnistria, raising the risk of periodic instability even as pro-EU control strengthens. Moldova will also face an elevated risk of cyberattacks aiming to undermine public trust in state institutions and the government.

The position of pro-Brussels actors will strengthen across the EU periphery in 2026. As Russia continues to suffer economically and the EU moves towards a complete ban on Russian hydrocarbons, Moscow will see a noticeable degradation of its political and economic leverage. While the ensuing shifts in political control across the region will prompt increased uncertainty in the medium term, late 2026 will likely see the establishment of a more stable status quo due to the consolidation of a broadly pro-EU consensus across the region. Despite the likely collapse of Russia's influence, Moscow will retain the ability to conduct low-cost cyber operations and misinformation campaigns that may have a significant impact on online discourse, the availability of public services, and the security of internet-based operations in affected countries.

Exterior view of the European Parliament.

AVIATION

ESCALATING CYBERSECURITY THREAT REQUIRES ADAPTIVE MEASURES

EXECUTIVE SUMMARY

As a cornerstone of global critical infrastructure, global aviation presents a complex cybersecurity landscape. The industry operates as one of the world's most intricate structural networks, spanning airlines, airports, suppliers, and regulators, all bound together by technology and human interface. Its complexity, visibility, and importance will therefore make it an attractive target for a broad spectrum of threat actors – from cybercriminals and hacktivists to state-sponsored groups and insider threats.

KEY JUDGMENTS

Aviation's vast interconnectivity – spanning airlines, suppliers, airports, and navigation systems – creates a complex cybersecurity environment and makes the sector an attractive target.

Cyberattacks are expanding in scale and sophistication, amplified by automation and AI, with impacts on data, finances, flight safety, communications, and supply chains.

Effective defense requires shared responsibility across stakeholders, balancing regulatory constraints with modernization, while strengthening resilience, training, recovery, and continuous improvements.

Human error and workforce shortages remain critical vulnerabilities.

Several large commercial aircraft parked on airport tarmac.

Threat Landscape

AVIATION'S GROWING EXPOSURE IN 2026

Global aviation operates as one of the world's most intricate structural networks, spanning airlines, airports, suppliers, and regulators, all bound together by technology and human interface. As a cornerstone of global critical infrastructure, the industry presents a complex cybersecurity landscape. Its visibility and importance make it an attractive target for a broad spectrum of threat actors – from cybercriminals and hacktivists to state-sponsored groups and insider threats.

The uneven momentum of technological upgrades and modernization, partly due to strict regulations designed to safeguard passengers, makes it more difficult for the industry to keep pace with a fast-evolving threat environment.

At the same time, the industry is becoming more interconnected, outsourced, and reliant on automation, digital systems, and AI. Airports, airlines, and third-party vendors increasingly share and manage data, while modern aircraft can exchange information in real time through systems like collision-avoidance technologies. AI-driven maintenance platforms now predict and schedule repairs with greater speed and accuracy.

Although these advances improve safety, efficiency, and capacity, they also expand the attack surface, increasing the potential for disruptions that cascade across every stage of aviation operations. Successful attacks can undermine finances, reputations, and the safety of air travel itself, while exposing passengers to data theft and travel disruptions.

AI AMPLIFIES THREATS

Cyberattacks within the last year have targeted nearly every corner of the aviation sector, from hacktivist campaigns against airlines, to app compromises, ransomware on suppliers, Distributed Denial-of-Service (DDoS) assaults on commercial websites, navigation jamming, and insider leaks of flight details. In September 2025, an attack on a check-in and boarding software provider disrupted operations at European airports – including London Heathrow, Berlin Brandenburg, Brussels, and Porto – demonstrating the risks of shared digital infrastructure across airlines.

The widespread availability and low cost of AI technology will amplify these threats, enabling both state-sponsored groups and low-level lone hackers to conduct faster, more effective attacks.

Common techniques such as malware, ransomware, and DDoS will persist. While some attacks seek to access sensitive information for financial gain, others aim to disrupt services, delay flights, promote political or social causes, or even create direct safety risks that threaten the continuity of air transport.

Passengers and enterprises face parallel risks. Hackers exploit public networks, spoof airline websites, and manipulate booking systems to steal financial and personal data. At the same time, the growing use of AI tools by travelers – whether for booking assistance or by entering sensitive details into platforms – creates new exposures for individuals and companies alike.

Air traffic control center at night.

AS PARTNERS AND NETWORKS GROW EVEN MORE INTERCONNECTED IN 2026, THE SECTOR WILL LIKELY FACE AN **ESCALATION OF CYBER THREATS,** INCLUDING NEW ATTACK TYPES WITH **POTENTIALLY GREATER IMPACTS**.

Cyberattacks	Technique	Likely Impact
DDOS ATTACKS	DDoS attacks on reservation systems	**Passenger disruption, revenue loss, reputational damage**
RANSOMWARE ATTACKS	Ransomware targeting operational IT	**Grounding of fleets, flight cancellations, safety risks**
APPLICATION COMPROMISE	Application compromise in critical systems	**Data theft, regulatory penalties, reputational damage**
SIGNAL JAMMING	Navigation signal jamming (GNSS interference)	**Flight delays, rerouting costs, increased fuel burn**
SUPPLIER BREACHES	Supplier or contractor breaches	**Cascade effects across airlines, airports, and regulators**

HUMAN ERROR PERSISTS

Despite advances in cybersecurity, human error will remain one of the primary vulnerabilities within aviation networks in 2026. Attackers are likely to continue exploiting people as the easiest entry point into critical systems, whether through phishing, credential theft, or social engineering.

Previous baseline security measures are no longer sufficient. Addressing human error will require stronger proactive and reactive strategies, including robust backup and recovery procedures to restore systems and data quickly after an incident. Multi-factor authentication (MFA), applied across enterprises and extended to traveler accounts, will strengthen access controls and help block unauthorized entry.

Workforce development – including training, retention, fatigue management, and continuous monitoring – will further strengthen defenses and reduce the likelihood of mistakes that undermine resilience.

Such measures, including embedding effective training and compliance requirements across the aviation sector, will not only strengthen resilience, but will also limit the likelihood of accidents, improving airline safety.

OUTLOOK

Implementing cybersecurity upgrades across aviation infrastructure, software, and firmware – while upholding uncompromising safety requirements – will be central to preventing future threats. Success will also depend on industry-wide collaboration, including the development of new standards, the updating of existing ones, and coordinated training across employees, organizations, governments, and vendors. Ensuring that all stakeholders are informed, trained, and compliant will be critical to building resilience.

Stronger Responses Required

COORDINATED ACTION ACROSS THE SECTOR

Effectively addressing cyber threats will require a coordinated, industry-wide response. Shared responsibility must extend across manufacturers, airlines, ground services, third-party vendors, and regulators, all of whom must align on standards, disclosure, and response coordination.

Stakeholders face a choice: proactively embed stronger cybersecurity into their operations, or continue risking ransomware demands, costly repairs, reputational damage, and potential safety compromises.

ADAPTING TO EVOLVING ATTACKS

Attack techniques are evolving rapidly, especially with the rise of AI. Defending against these threats will require stronger, coordinated proactive and reactive measures. Best practices must align with international cybersecurity standards and be applied consistently at both enterprise and individual levels. Training, education, and continuous adoption of modern security tools will be critical to reduce vulnerabilities and build sector-wide resilience.

SECURING OT ENVIRONMENTS

Operational Technology (OT) systems – including aircraft, ground control, and baggage handling – require distinct protections. Effective strategies include network segmentation, protocol monitoring, endpoint protection, strict access controls, and limited remote access. OT environments are often harder to secure due to legacy hardware and proprietary protocols, but the safety implications of disruption make dedicated, integrated cyber controls essential.

SIGNALS TO WATCH

- → The growth in state-sponsored cyber probes targeting OT systems.
- → Introduction of new ICAO or FAA sustainability rules with operational impacts.
- → Unusual patterns of GNSS jamming or spoofing in contested regions.

RECOMMENDED ACTIONS

Program-Level Actions

- Modernize cyber resilience programs, with clear integration between IT and OT security.
- Expand joint threat intelligence sharing with government and industry peers.
- Invest in workforce development, training, and retention to reduce human error risks.

Day-to-Day Measures

- Segment IT and OT networks to contain breaches.
- Audit vendor and supplier security practices regularly.
- Enhance incident response playbooks, and conduct frequent tabletop drills.

Plane on runway taking off.

ASIA-PACIFIC

EXECUTIVE SUMMARY

Sino-American competition and US policy uncertainty are pushing Asia-Pacific governments towards heightened nationalism, protectionism, and rearmament, making brief, localized crises at sea and along disputed borders likely through 2026. Tensions will persist between Taipei and Beijing, falling short of direct confrontation. Maritime flashpoints in the South China Sea and Taiwan Strait – and sporadic land-border clashes in South and Southeast Asia – will periodically disrupt sea lines of communication (SLOCs), overland routes, and travel, keeping freight and insurance costs elevated. Parallel trade frictions, resource nationalism, and election-season politics will likely amplify regulatory volatility, protests, and brand risk.

EVENTS TO WATCH

- **South China Sea/Taiwan Strait collision or coercive intercept:** A major at-sea incident (e.g., ramming, water-cannoning, close-range intercept) could prompt short, partial SLOC closures and rerouting – delaying freight for weeks, spiking insurance premiums, and snarling access to the Strait of Malacca.
- **China's revised data rules effective January 1, 2026:** Stricter cross-border transfer reviews, localization obligations, and executive liability could raise compliance costs and regulatory exposure – prompting firms to review data flows, adjust travel policies, and harden governance measures.
- **Thailand's March 2026 election amid Thailand-Cambodia border tensions:** Hardline campaign rhetoric or breakdowns in talks could reignite clashes near disputed temples, trigger border crossing closures, disrupt portal/rail corridors, and constrain staffing and travel in border provinces.

KEY JUDGMENTS

Tensions will persist between Taipei and Beijing, falling short of direct confrontation, as Beijing prioritizes non-military tactics, and direct engagement from extra-regional players remains unlikely.

Security incidents and close calls will occur around temporary SLOCs and along busy airline corridors where the ongoing regional arms buildup raises the risk of miscalculation.

Unresolved territorial disputes, particularly in South and Southeast Asia, will likely cause intermittent border closures and cargo/travel delays amid a sustained risk of limited military conflict.

Rising global trade competition and nationalism will likely fuel unrest in already unstable states, triggering regulatory swings and brand reputation risks.

The Jinshanling section of the Great Wall of China.

South China Sea and Taiwan Strait: Maritime Escalation Risk Likely to Rise

An accelerating arms buildup and shifting strategic alignments, largely designed to deter China, are likely to raise escalation risk in the South China Sea and Taiwan Strait through 2026. This climate will likely provoke localized standoffs that disrupt SLOCs, if only temporarily, raising shipping and insurance costs, and chilling capital flows.

An ongoing arms race will keep the Taiwan Strait and South China Sea at the forefront of potential destabilization. Defense spending across Asia has risen over the last decade, driven by US policy uncertainty, regional threat perceptions, and capabilities races. Washington has called on key partners – especially Japan, South Korea, and Taiwan – to raise defense spending to 5 percent of their Gross Domestic Products (GDP). Although this target will not be met, overall defense budgets will rise. Their prioritization of anti-missile and counter-drone systems will continue, while Southeast Asian countries focus on defensive capabilities and training as key regional actors, such as Beijing, expand naval capacity.

SOUTH CHINA SEA

China's maritime assertiveness in the South China Sea will continue due to the strategic proximity, importance, and the commercial value of its SLOCs. This will take the form of a more visible military and infrastructural presence, increased patrols, and diplomatic flare-ups with claimant states. While a major or sustained conflict is unlikely, triggers heightening the risk of a limited escalation in 2026 include: assertive joint maritime patrols or facilitated naval transits involving the US and Indo-Pacific Middle Powers (Australia, Japan, South Korea), a buildup of perceived military infrastructure on reclaimed land, and unilateral energy exploration projects in disputed waters.

Hotspots around Scarborough Shoal and the Spratly Islands remain the most vulnerable to confrontations that drive route volatility, regulatory compliance challenges, and shipping delays.

Prolonged or direct conflict is unlikely, but naval standoffs and possible partial SLOC closures could follow serious collisions or unprecedented force during high-risk maneuvers like close-range intercepts, blocking runs, chases, or water-cannon use. Disruptions – especially due to spillover effects like blockades or sea denial exercises affecting access to the adjacent Strait of Malacca – could delay commercial freight for several weeks in extreme cases, and prompt further security-force expansion in disputed waters.

The risk of a major or sustained conflict is mitigated by a range of factors, including China's longer-term diplomatic goals and close economic ties with multiple regional states. Ties are set to grow as China competes with the US to expand its influence through trade agreements like the ASEAN-China Free Trade Area (ACFTA) 3.0 Upgrade Protocol. The Association of South East Asian Nations (ASEAN), as a regional bloc, will also be motivated to offer quick de-escalation pathways through talks and redirection to international institutions. ASEAN capitals face the challenge of balancing practical realities of China's military capabilities, the need for economic ties with multiple powers, upheaval in US policy, and the desire to maintain a degree of autonomy in foreign and trade policies outside the bloc. These dynamics lower the likelihood of sustained escalation.

TAIWAN STRAIT

Tensions will persist in the coming year between Taipei and Beijing, although direct confrontation is unlikely, as Beijing prioritizes non-military tactics, such as economic pressure and influence operations under the "three warfares" strategy, to achieve its stated aim of peaceful reunification. Economic inducement will mainly target businesses that would profit from the Chinese market, e-commerce and logistics chains, as well as capital routed through proxies in Hong Kong. Public opinion, particularly among Taiwanese youth, is typically shaped by exploiting existing political and/or cultural sympathies towards Beijing and capitalizing on increased uncertainty in US foreign policy. Expansion of countermeasures to displace Beijing's messaging, such as increased media and political funding scrutiny, is limited by Taipei's desire to disassociate from an authoritarian past.

Nevertheless, Taipei continues to strengthen its military deterrence – prioritizing US naval systems, F-16 combat aircraft upgrades, and drone/anti-drone capabilities. Further US arms sales could be delayed or withheld if Washington seeks further trade talks with Beijing.

Deterrent naval exercises will likely increase for Beijing, Washington, and their allies; live-fire drills, arms procurement, or large-scale military exercises will be perceived as serious provocations. Military incidents – such as naval collisions or unprecedented airspace intrusions – are most likely triggers for limited open-water confrontations, though strategic calculus in Beijing and Taipei would deter a prolonged, highly disruptive conflict.

Direct involvement of extra regional actors remains unlikely, and simultaneous conflicts in the South China Sea or Taiwan Strait remain low risk. Still, security or diplomatic incidents in either theater will likely prompt limited, regional escalations – such as increased naval blockades or military buildups lasting several weeks – followed by talks facilitated by international partners leading to gradual de-escalation. Business impacts (e.g., supply chain disruptions) will likely persist for at least four weeks after normalization as operators clear rerouted cargo backlogs; commercial shipping costs will likely stay elevated due to higher insurance premiums and precautionary rerouting. Nationalist sentiment can also drive reputational risk for foreign entities during spikes in tensions.

Cargo ship navigates South China Sea.

Impacts of Ongoing Border Disputes to Persist in South and Southeast Asia

Disputed borders will be flashpoints for violence through 2026 as governments and non-state actors use tactics short of open warfare to press their agendas, placing businesses and travelers operating in these areas at risk of recurrent disruption. Expect sporadic clashes, sabotage operations, and cyberattacks that disrupt logistics networks, delay cross-border travel, and increase insurance and security expenses. Territorial disputes between neighbors persist across the region, especially in three key areas:

- **India-Pakistan:** Periodic Line of Control (LoC) flare-ups and grey-zone actions will worsen already severely limited bilateral trade and transit routes. Sporadic terrorist attacks will continue in Pakistan and major urban centers in India's north.
- **Afghanistan-Pakistan:** Retaliatory cross-border fire and airstrikes against militants will likely complicate the movement of essential supplies to landlocked Afghanistan and heighten the risk of targeted and incidental violence affecting foreign entities.
- **Thailand-Cambodia:** Localized border clashes will continue to restrict cross-border trade amid heightened nationalist sentiments that could impact staffing and travel plans.

INDIA-PAKISTAN

Businesses in border districts, including the LoC in the Kashmir region, will face elevated risk of direct and grey-zone conflict through 2026. The fallout from the May 2025 clashes along the Kashmir border included New Delhi's political decision to eliminate distinctions between non-state actors and their state sponsors, raising the prospect of broader retaliation in the future. Nuclear deterrence will mitigate the risk of conventional war. However, sabotage operations targeting infrastructure and military installations, limited cyberattacks on logistics networks, disinformation campaigns, and the use of proxies for terror attacks will continue.

Domestic politics will add friction: ahead of state elections scheduled for the first half of 2026, Indian officials will attribute anti-government and communal violence to Pakistan. Following the 2025 escalation, India withdrew from the Indus River Water Treaty, heightening water-security concerns in Pakistan and fueling both hydro-nationalism and public pressure for a tougher stance against India. With bilateral de-escalation channels weakened, troop altercations along the LoC could quickly escalate into limited standoffs. Other triggers for escalation include new dams or diversion projects by India that reduce Indus River water supply to Pakistan, mass-casualty terrorist attacks that Indian authorities link to Pakistani entities or vice versa, provocative military exercises near disputed areas, and cyber operations disrupting critical infrastructure.

AFGHANISTAN-PAKISTAN

The Durand Line – the disputed border between Afghanistan and Pakistan – will remain a high-risk zone for cargo transport and cross-border operations through 2026. Both sides accuse the other of enabling militant groups. Full-blown war is unlikely; however, recurrent limited conflicts – cross-border fire and airstrikes – are likely. Mass-casualty attacks in major Pakistani cities by the Tehreek-e-Taliban Pakistan (TTP) – which Pakistan links to the Afghan Taliban – are the most probable triggers for Pakistani cross-border security operations and possible Afghan retaliation. Intermittent border closures in 2025 have reduced bilateral trade from USD 2.5 billion to USD 1 billion, with further disruptions likely to impact the supply of food, fuel, pharmaceuticals, and construction materials to Afghanistan.

The threat of terror attacks will remain extreme, especially for foreigners in border regions. Chinese entities operating in Balochistan and Khyber Pakhtunkhwa – particularly those tied to China-Pakistan Economic Corridor (CPEC) projects – face heightened risks from anti-government groups, including separatists and Islamist militants. Expect periodic freight pauses, route diversions, and added security costs following incidents.

THAILAND-CAMBODIA

Sustained cross-border disruptions are likely through 2026. The July 2025 border clashes around disputed temple areas – including Preah Vihear – caused dozens of casualties and displaced 300,000 people. While negotiations continue, a near-term resolution is unlikely. Although both sides have agreed to a phased withdrawal of heavy weaponry through February 2026, sporadic border skirmishes persist, and flare-up risks along the border remain high.

Nationalist sentiment in both countries has fueled attacks on minorities – Thais and Cambodians – and on Chinese and Laotians via misidentification, straining factory staffing in border provinces. With Thailand expected to hold elections in early 2026, anti-Cambodian rhetoric and disinformation targeting Thai voters will rise. The polls will involve a considerable pool of undecided voters, whose trust political parties are likely to seek by promising strong leadership and evoking nationalistic rhetoric. The Bhumjaithai party is best placed to win due to its pragmatic approach in partnering with both conservative parties that are unpopular with youth and progressive parties that have faced multiple political and legal challenges in forming a majority government. Any incoming leader is likely to pursue a gradual and conditional restoration of ties with Cambodia although permanent resolution to territorial disputes is unlikely.

Closures at key crossings and tighter checks are already disrupting Southeast Asia's port and rail corridors, with reported closures affecting over USD 848 million in trade per month. Vietnamese firms are reassessing goods movement through Thailand and Cambodia, and more companies will likely reevaluate exposure to Cambodian-produced goods, including metal works worth over USD 628 million. Travel to temple sites along the border remains vulnerable to intermittent restrictions and heightened screening. Renewed clashes causing multiple injuries or the breakdown of negotiations – particularly if accompanied by hardline campaign rhetoric – would likely trigger new flare-ups and prolonged disruptions.

Afghan refugees returning from Pakistan, November 2023.

Trade Competition, Resource Nationalism, and Rising Geopolitical Frictions

US-China trade competition remains a key manifestation of broader geopolitical rivalry, with Southeast and South Asia among the most exposed to impacts. Businesses operating in or relying on supply chains routed through the region can expect ongoing disruption related to fluid trade policies, implementation, and regulatory challenges. Flexibility and optionality will aid organizations in navigating this complex dynamic.

Decoupling of the American and Chinese economies is improbable given China's cost advantages in production, and necessity to retain its central role in global manufacturing to utilize its overcapacity in several sectors. Moreover, despite Washington's threats, most Chinese exports to the US will attract a tariff that is lower than countries seen as potential reshoring destinations like India. Hence, supply chain de-risking using a 'China plus one' strategy – placing operations in China and one other location with lower US trade barriers or maintaining isolated supply chains for China and US-allied countries – is only pragmatic for large firms in sectors considered vulnerable to fresh trade curbs. These include industries dependent on critical minerals like battery, electric vehicle, and industrial machinery production, advanced and dual-use technology such as aerospace and defense semiconductors, microelectronics, AI, and quantum computing, as well as consumer goods that rely on labor-intensive manufacturing and/or assembly in China.

Governments are also leaning into resource nationalism and protectionism under pressure from major powers, like the US and China. Changes to raw mineral export restrictions and recent deals, including between Australia and the US, underscore how critical resources are being used as strategic tools. Spillovers beyond trade are likely: states may step up military posturing in contested areas like the South China Sea, where strategic resources and major shipping routes overlap. Competition to secure resources, processing capacity, and supporting logistics infrastructure will likely increase policy volatility, regulatory shifts, and supply-chain disruptions as governments prioritize domestic control of key sectors.

NATIONALISM, POLITICAL INSTABILITY, AND HEIGHTENED THREAT FROM UNREST

Nationalism – and rising far-right and anti-immigration sentiment – will likely remain a key driver of domestic politics across Asia-Pacific through 2026. In 2025, Australia saw anti-immigration rallies involving far-right and neo-Nazi elements; Japan's populist Japan First party expanded its upper-house presence on a platform of stricter immigration; and in South Korea, nationalist and far-right narratives alleging Chinese interference in the impeachment of former President Yoon Seok-yeol and the subsequent election fueled anti-Chinese sentiment and bilateral friction.

Anti-immigrant rallies in Australia reflect the growing traction of far-right and nationalist rhetoric in domestic politics.

Nationalism has also coincided with small-scale targeted violence. In 2025, lone attackers targeting Japanese nationals in China were attributed to nationalist motives. In Japan, assaults on Chinese residents occurred amid anti-foreigner campaigns led by Japan First. Likewise, South Korea witnessed violent incidents tied to anti-Chinese sentiment. For businesses, these dynamics can translate into tighter curbs on foreign labor, reputational risk, and increased security requirements for expatriates and foreign-linked assets.

Regulatory standards and scrutiny for foreign entities will also intensify, aiming to address local grievances and ensure compliance with country-specific rules. Beijing will further revise its data protection laws effective January 1, 2026, increasing data storage, governance, and transfer costs due to mandatory regulator-led reviews or a third-party certification with continuous auditor reviews for cross-border data sharing, data localization, and appointment of a data protection officer to handle large amounts of data. Notably, company executives are also deemed liable and can be fined or tried in criminal cases warranting detention or exit bans. Ethnic Chinese and/or dual nationals, as well as citizens of US and allied nations like Japan, remain at highest risk of cases under national security or other local laws, especially during periods of heightened diplomatic tensions over military exercises and trade negotiations.

Violent protests have raised public scrutiny of Indonesian President Prabowo Subianto, raising the likelihood of further unrest and policy concessions in 2026.

ELECTIONS, LEADERSHIP TRANSITIONS, AND ELEVATED POLITICAL VIOLENCE

Against a backdrop of geopolitical tensions and economic uncertainty, elections and leadership shifts across Asia will likely increase political instability and associated violence through 2026. Expect protest surges around campaign milestones, court rulings, and policy announcements. Resultant measures like periodic curfews, telecommuting advisories, and security cordons are likely to cause intermittent disruptions to travel and last-mile logistics in affected capitals and provincial hubs.

Bangladesh: The interim government's 2025 ban of the Awami League (AL) under terrorism legislation has created a political vacuum that has strengthened conservative Islamist factions. Risks of minority discrimination and impactful unrest will likely rise as former AL supporters organize, and Islamist parties mobilize, ahead of the mid-February 2026 elections.

Indonesia: Following violent and disruptive protests over lawmakers' perks and perceived corruption, President Prabowo Subianto modified his cabinet and amended laws broadening the military's roles in civilian affairs in moves that will likely fall short of frustrated citizen expectations. Student groups have set an August 2026 deadline for key institutional reforms, raising the likelihood of fresh demonstrations if demands are unmet.

Myanmar: Delayed elections, slated to begin December 2025 and continue through early 2026, are unlikely to deliver stability or a legitimate government – and could trigger further conflict amid limited military control and persistent anti-junta armed resistance.

Thailand: The March 2026 general election will test declining support for traditionally powerful parties like the Pheu Thai and Bhumjaithai Party. Rising nationalist sentiment and fragmented coalitions are likely to delay government formation after what will likely be a peaceful vote, and we expect moderate political instability through 2026.

MIDDLE EAST & NORTH AFRICA

EXECUTIVE SUMMARY

In 2026, the Middle East's security environment will be shaped by the enduring consequences of the Israel-Hamas conflict. A US-brokered ceasefire has reduced large-scale fighting but remains fragile as Israeli-Palestinian tensions and rivalries among Arab states persist. Over the past two years, this confrontation has redefined the regional power dynamics and disrupted the prior grey-zone equilibrium, weighing on travel, supply chains, and operational resilience. Meanwhile, North Africa – though relatively less affected by these shocks – will continue to face internal instability and a drift toward greater autocracy even as business interest grows.

EVENTS TO WATCH:

- **Iran-Israel re-escalation (multi-day direct strikes):** Direct exchanges will likely force regional flight cancellations and reroutes, slow traffic at maritime choke points, disrupt energy flows, and drive broad business interruptions across the Middle East.
- **Lebanon 2026, UNIFIL exit and Hizballah disarmament test:** UNIFIL's departure and a contested Lebanese Hizballah (LH) disarmament process raise clash and spillover risks, tightening travel and operating postures in and around Beirut.
- **Israel political timeline amid isolation (election by Oct 27):** Campaigning while Gaza remains unresolved will intensify domestic unrest and widen global protests/boycotts, elevating brand, travel, and compliance risks.

KEY JUDGMENTS

The Israel-Hamas conflict and Iran-Israel balancing act will continue to influence the region's geopolitical and security landscape.

Further direct Iran-Israel conflict will cause recurring travel, supply chain, and business disruption.

Failure to secure peace in Gaza will likely deepen Israel's diplomatic isolation and spur protests and boycotts.

North Africa, though less affected, is likely to remain unstable and more autocratic, even as businesses pursue new opportunities in the region.

Al-Aqsa Mosque at night in Jerusalem, Israel.

Persisting Israel-Hamas Conflict to Shape Middle Eastern Geopolitics

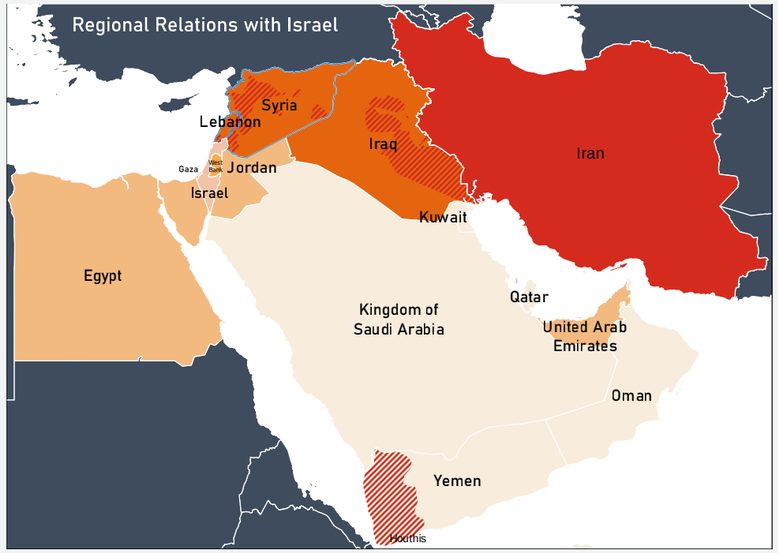
LIMITS OF DIPLOMACY

Despite renewed diplomatic efforts, including the strained ceasefire and US President Donald Trump's UN-approved 20 Point Peace Plan, Israel – while voicing support for talks – will likely continue to move away from diplomatic negotiations and prioritize military operations to assert full control over Gaza and the West Bank. Likely ceasefire violations and continued cross-border attacks from both sides will allow Israel to argue that only a military option can secure long-term control, further eroding confidence in negotiated solutions. This strategy reflects Prime Minister Benjamin Netanyahu's "day after" vision for Gaza's future. Rejecting a Palestinian Authority-led pathway to statehood, Netanyahu is relying on the US-backed Gaza Reconstitution, Economic Acceleration and Transformation (GREAT) plan and its Board of Peace. These projects – likened to a Trump Riviera – would require the departure of a quarter of Gaza's population. Despite widespread international criticism, Israel and the US will likely continue advancing their strategic vision for the Middle East.

International diplomacy will endure despite headwinds, likely further isolating Israel and the US as their preferred settlement entails the displacement of Palestinians. In September 2025, at the UN General Assembly, dozens of Western governments – including Australia, Canada, France, and the UK – officially recognized Palestine. The UN General Assembly also backed a French-Saudi proposal envisioning a permanent ceasefire and the release of all hostages, followed by reconstruction under a UN civilian and security support mission working with Palestinian authorities, with Israel's consent. Israel and the US did not consider the proposal, and US veto power makes Security Council approval unlikely. In lieu of this proposal, the UN Security Council on Nov. 18 passed a US-drafted resolution in support of Trump's peace plan for Gaza. The proposal implies an eventual independent Palestinian state, but gives no timeline nor guarantees, even as it expresses support for the deployment of a stabilization force in Gaza.

Recognition of a Palestinian state and the new UN peace plan will therefore remain largely symbolic, underscoring collapsed mediation and a drift back into confrontation. Although recognition aims to pressure Israel toward a diplomatic solution, it will likely have the opposite effect. If Netanyahu continues a retaliatory strategy of fully annexing the West Bank and Gaza to block a future Palestinian state, Israel will grow more isolated in 2026, with the US its only highly visible ally. Rising isolation will complicate US-led peacemaking, embolden anti-Western narratives, and heighten the risk of renewed regional escalation.

In 2026, more countries could recognize the State of Palestine, denouncing Israel's operations in the Palestinian Territories and advocating for a two-state solution.



UN vehicle in southern Lebanon.

ISRAEL'S INCREASING ISOLATION

Israel has shifted its long-standing security paradigm of limited deterrence to a maximalist strategy that targets Iran's proxies – regardless of host country – and directly striking Iran. This change has intensified regional volatility and pushed Arab states and Europe to increasingly view Israel as a destabilizing and pariah-like state. Arab governments once fixated on Iran's nuclear ambitions and regional militias now see Israel's multifront conflict as a significant long-term threat to stability. Israel's approach also conflicts the Gulf Cooperation Council (GCC) priorities to protect economic growth. Before the October 7 attacks – and even amid the Israel-Hamas war – speculation about expanding the Abraham Accords to Saudi Arabia, Syria, and Lebanon was widespread. Israel's September strike on a Hamas apartment in Qatar likely set back the likelihood of further Gulf State-Israel normalization agreements in 2026, absent maximalist US prodding and an unexpected breakthrough toward a more enduring peace between Israel and Hamas.

Israel is under more diplomatic pressure, particularly from European states. Although many public statements are aimed at domestic consumption, some have taken a stronger stance. Madrid cancelled a USD 825 million arms deal in September and is proposing a ban on all military equipment sales or purchases with Israel due to the Gaza conflict. Türkiye declared Israel a "terror state," cutting off direct trade ties in May 2024 and closing its airspace to Israeli aircraft in August 2025. In September 2025, the European Commission proposed unprecedented measures, including suspending trade concessions and applying sanctions to extremist ministers amid rising public pressure. Diplomatic pressure will likely increase in 2026, and the growing perception of Israel as a pariah within the international community – even if largely rhetorical – will contribute to a rise in anti-war and anti-Israeli protests and boycotts across the globe.

At home, former prime ministers have accused Netanyahu of making Israel a pariah. A growing sense of international isolation will almost certainly intensify civil unrest opposing Netanyahu ahead of national elections due by Oct. 27, 2026, though an early vote remains possible. Netanyahu's candidacy and election timing will hinge on the perceived Gaza outcome and the stability of his governing coalition. Israel is increasingly perceived as a destabilizing force in the Middle East and a state facing mounting international marginalization, even as domestic dissatisfaction grows. Absent a diplomatic resolution to the Israel-Hamas conflict – and, by extension, the Israel-Palestine issue – its isolation is likely to intensify, particularly as Israel appears willing to disregard international law in favor of military force.

Iran-Israel Balancing Act to Determine Regional Power Dynamics

IRAN-ISRAEL: POSSIBLE SCENARIOS

The June 2025, 12-day war between Israel and Iran marked a major escalation in their long-standing rivalry and underscored the risk of future conflict. In 2026, three possible scenarios will shape their relationship and stability in the region.

SCENARIO 1

Direct War Resumes: Highly Destabilizing (Moderate Likelihood)

Another direct war would likely follow a similar trajectory to the first conflict, escalating the longer it endures. It would upend energy markets, disrupt maritime trade routes, and severely undermine efforts to stabilize regional economies.

As Iran rebuilds its nuclear and military capabilities under international sanctions – refusing to suspend its enrichment program – the US and Israel would renew their air campaign against strategic sites in Iran. In turn, Iran would resume strikes against Israel and US assets in the region, directly or via proxies. This would heighten regional instability and could ignite a full-scale regional war as other participants – such as Lebanon and GCC countries – are drawn in. Impacts for organizations would mirror the 12-day war: kinetic risks in Israel and Iran; widespread travel disruption and business interruption across the Middle East; and additional impacts on global trade and logistics. While many international actors, including the E3 (UK, France, and Germany), are still negotiating to reach a new Iran nuclear deal that will avoid this scenario, diplomacy has yielded little. On Sept. 27, the UN reimposed "snapback" sanctions on Iran. If stakeholders cannot find room for diplomacy, this destabilizing scenario could define the Middle East in 2026.

On Sept. 15, Qatar hosted an emergency Islamic Summit to condemn Israel's Sept. 9 strike on Doha.

SCENARIO 2

New Nuclear Agreement Reached: More Stable (Low Likelihood)

Announcing snapback sanctions, US Secretary of State Marco Rubio stated that "diplomacy is still an option" and that "direct talks" should resume. Talks resulting in a new nuclear deal would create a more stable environment in 2026. However, trust remains a major obstacle: any Iranian proposal to resume talks relies on Washington and Tel Aviv refraining from additional strikes against Iran – terms the US will most likely not accept.

SCENARIO 3

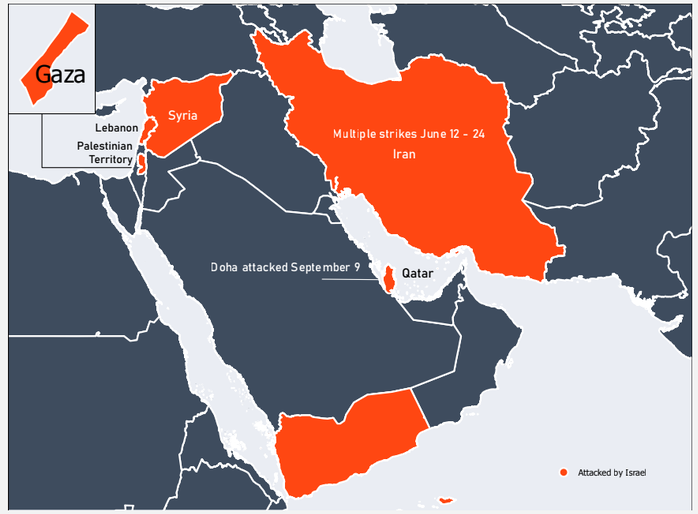
Grey-Zone Status Quo Returns: Ongoing Instability (Most Likely)

Iran and Israel would resume grey-zone conflict, relying on proxies, cyber tactics, and covert operations to destabilize each other. Violence would remain cyclical and at times intense but stop short of full-scale war. Iran is likely to maintain this posture, combining limited tactical diplomacy with the West – which yields little substantive progress but keeps communication channels open – while continuing to rebuild its military and nuclear capabilities. Persistent grey-zone warfare will sustain strategic uncertainty, elevating political and operational risks for international actors in the region. Israel would continue targeted strikes on Iranian assets and proxies across the Middle East, and periodic flare-ups – similar to the June 2025 conflict – would remain a real risk. Iranian-backed actors, including Shi'a militias in Iraq, Lebanese Hizballah (LH), and Yemen's Al-Houthis, would also continue to destabilize neighboring states.

LEBANON, SYRIA: TORN BETWEEN IRAN AND ISRAEL

The military defeat of Iran's Axis of Resistance enabled major geopolitical shifts – including the fall of the al-Assad regime in December 2024 – but Iran's influence will endure through 2026, as the complex disarmament process of LH shows. The Lebanese government adopted a phased plan in early September 2025; it faces significant hurdles, especially in LH strongholds in the Beqa'a Valley and Dahieh. LH and Iran have condemned this plan, leaving Beirut caught between LH-aligned factions and US/Israeli pressure conditioning aid and security guarantees on LH's full disarmament.

Israel shifted military strategy, targeting Iran and its proxies directly throughout the region.



Lebanon 2026. The year will likely be a turning point for LH's influence and a major test for the Lebanese Armed Forces (LAF). Beyond disarming LH, the LAF must replace the UN Interim Force in Lebanon (UNIFIL), which plans to depart after 48 years. Under President Joseph Aoun, the LAF and government must assert authority, maintain national unity, and ensure security across the country. This will be essential not only for internal stability but also to prevent Lebanon from being further drawn into escalating tensions between Iran and Israel.

Syria 2026. Interim President Ahmed Al Sharaa's new government will need to prove its ability to unify and control territory that remains fundamentally divided along communal lines. Grappling with ethnic violence, Al Sharaa will need to assert government authority, develop a security apparatus trusted by all Syrians, and rebuild a country torn by 15 years of war. Should Al Sharaa fail to reassert central control over the country, Syria will likely continue to face inter-communal clashes and growing civil unrest, posing a credible risk to organizations considering a return to the country. This task is further complicated by Israel's ambitions in the Golan Heights, as Tel Aviv seizes territory and creates new buffer zones along the shared border.

Al Sharaa is pursuing a conciliatory approach opting not to respond to regular Israeli airstrikes on Syrian territory and instead engaging in negotiations over a potential security agreement with Israel. This strategy may reduce immediate tensions but risks undermining Syria's territorial integrity – particularly along its southwestern border – and eroding state authority. It also gives leverage to opposition groups, including a resurgent Islamic State (IS), seeking to rebuild its caliphate. The situation remains contingent on US policy, as renewed diplomatic engagement could delay, but not eliminate, a future troop drawdown. Any shift in Washington's posture will shape security conditions and the balance of power among armed groups through 2026.

ECONOMIC IMPACT OF IRAN-ISRAEL TENSIONS ON THE GULF

The Gulf States face extended uncertainty as Iran-Israel hostility persists, posing a substantial risk to economic growth. Iran's June strike in Qatar jeopardized the Gulf's reputation as a bastion of relative stability, exposing its vulnerability and shaking investor confidence in the region's role as a reliable economic hub and a secure environment for global commerce.

Conflict once implausible now appears real for Gulf stability and critical infrastructure. After the Iranian and Israeli strikes on Qatar, the safe-haven perception is increasingly at risk. A contained conflict and durable cold peace could restore some confidence, but another major strike – particularly on ports, refineries, or government infrastructure – would likely irreparably damage the Gulf's reputation as a secure, stable hub. If instability continues into 2026, long-term strategies built on an assumption of a stable and prosperous Gulf will begin to unravel. Eroding investor confidence and perceptions of insecurity in the Gulf could have global economic implications, particularly for energy markets and foreign direct investment flows.

North Africa: Characterized by Instability and Autocracy

As Middle East instability grows, global attention is shifting to North Africa, perceived as relatively more stable. However, while the Maghreb remains relatively unscathed by the Israel-Hamas conflict, its security environment is highly volatile. Algeria, Egypt, and Tunisia are intensifying crackdowns on opposition figures, stoking civil unrest, and leaning further toward autocratic governance. This erosion of democratic freedoms – coupled with worsening economic conditions – raises the risk of renewed civil unrest, potentially disrupting business operations and complicating compliance decisions across the region.

Libya exemplifies the tension between growing international interest and ongoing volatility. Increasing global attention to Libya's oil sector signals some confidence in its security environment, but the country remains deeply divided, with rival governments and numerous militias competing for control. This fragmentation creates significant challenges for investors, as control over oil resources is contested among armed groups and political factions. Consequently, despite rising interest, investing in Libya's oil industry and operating in Libya involves non-negligible risks – not only in terms of security but also in navigating local politics and legal processes.

Businesses operating in Libya face serious risks from protests that can block roads and from armed clashes between rival groups that cause collateral damage. Kidnapping for ransom – opportunistic or politically motivated – remains a severe threat. Companies should enforce strict security protocols to protect personnel on the ground. Navigating Libya's complicated political and administrative landscape often requires support from vetted, on-the-ground networks with the knowledge and contacts to enable market entry and expansion.

Seafront-skyline view of Libyan capital of Tripoli.

MARITIME

TRADE POLICY TO DISRUPT SHIPPING THROUGH 2026

EXECUTIVE SUMMARY

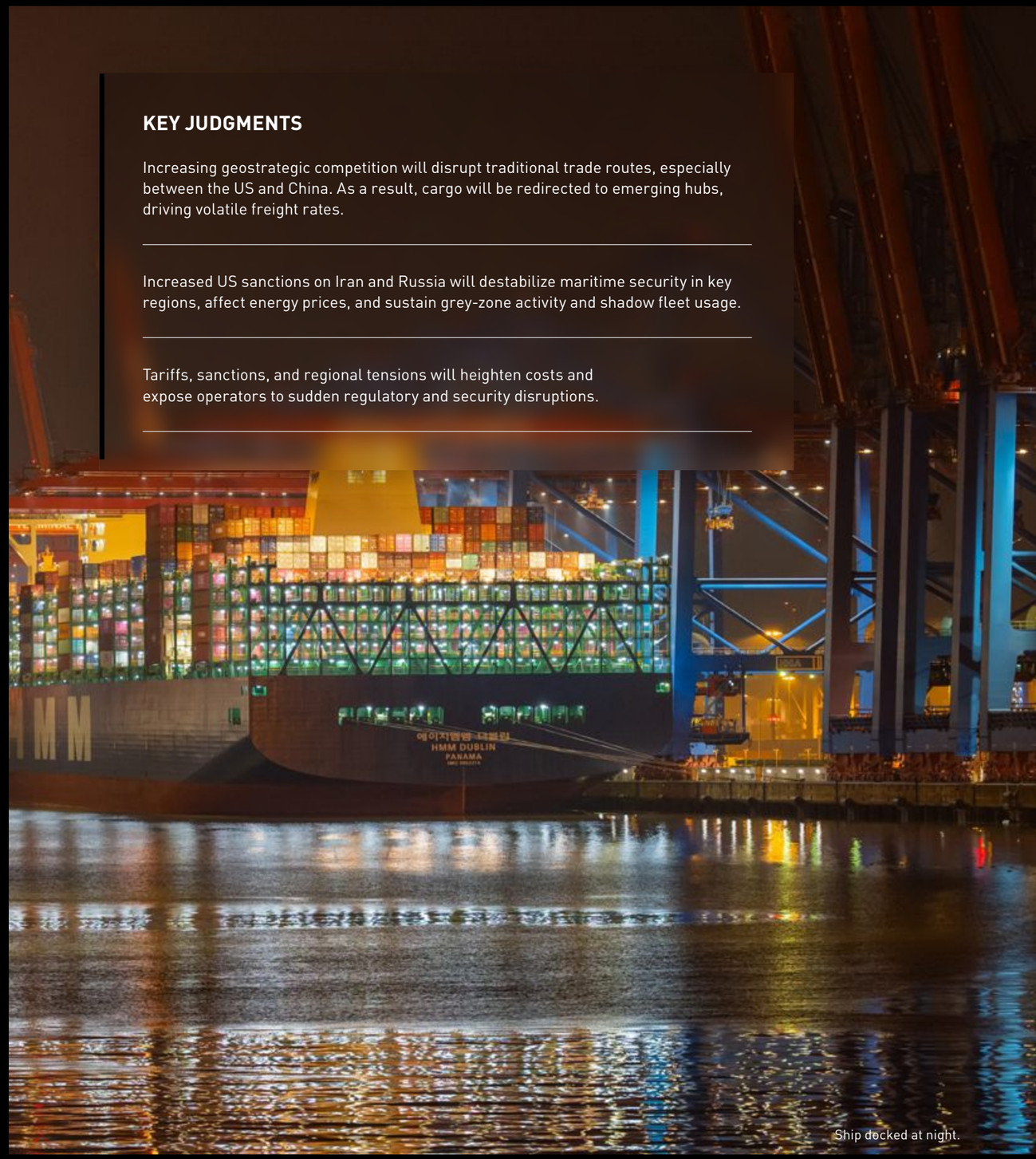
Intensifying geostrategic competition will have significant impacts on maritime trade and security in 2026. Tariffs and fees aimed at promoting domestic production and shipbuilding will particularly affect trade routes between China and the Americas, while US foreign policy towards Iran and Russia, among other countries, has the potential to impact energy markets and maritime security globally. Together, these forces will raise costs, disrupt trade patterns, and increase uncertainty for operators worldwide.

KEY JUDGMENTS

Increasing geostrategic competition will disrupt traditional trade routes, especially between the US and China. As a result, cargo will be redirected to emerging hubs, driving volatile freight rates.

Increased US sanctions on Iran and Russia will destabilize maritime security in key regions, affect energy prices, and sustain grey-zone activity and shadow fleet usage.

Tariffs, sanctions, and regional tensions will heighten costs and expose operators to sudden regulatory and security disruptions.



Ship docked at night.

Threat Landscape

TARIFFS TO RESHAPE SHIPPING PATTERNS

Since January 2025, the US has frequently threatened, imposed, retracted, and reinstated tariffs. While all measures affect trade, uncertainty over tariffs or their implementation on Chinese goods and fees on Chinese ships entering US ports are most likely to disrupt traditional sea routes, push cargo toward alternative ports, and lead to volatile shipping costs.

Companies may redirect sourcing to Southeast Asia or Latin America. Operators using Chinese-built vessels could re-route cargo through regional ports and complete journeys by land. These shifts will increase traffic on secondary routes, lengthen delivery times, and add supply chain complexity.

Such adjustments will ease pressure on some major ports but overload secondary and transshipment hubs. Congestion at these facilities will slow turnaround times; in the long run, however, bottlenecks could spur investment and strengthen regional hubs. Freight markets will remain unpredictable – tariffs will supress trans-Pacific traffic, but sudden pauses or rollbacks could trigger temporary surges.

Attempts to bypass tariffs – through ship-to-ship transfers, flag hopping, or concealing cargo origins via third-country ports – pose additional risks. Such practices raise safety hazards, legal exposure, and reputational costs while increasing the chance for further sanctions.

Overall, the threat of tariffs introduces structural uncertainty into global shipping networks. Operators must contend with abrupt regulatory shifts, complex logistics, and rising compliance costs – pressures that will reverberate through supply chains throughout 2026.

SANCTIONS, SHADOW FLEETS, AND CHOKEPOINT RISKS

US policy toward Iran and Russia is shaped by pressure and limited engagement – treating both as systemic rivals while avoiding large military commitments and instead relying on economic and diplomatic tools.

Iran's Escalation Risks

In Iran's case, this pressure will likely take the form of ramping up "maximum pressure" sanctions aimed at energy exports, state-owned companies, and shipping firms. Tehran's response is expected to be calculated rather than reckless, with further maritime incidents probable in 2026 within the framework of the decades-long grey-zone conflict.

Tehran has little appetite for immediate confrontation, but the longer sanctions endure, and the deeper their impact, the greater the pressure to retaliate. Maritime harassment and tit-for-tat tanker seizures are the most likely outcomes. In more severe scenarios, Iran could employ limpet mines in the Persian Gulf or UAV strikes in the Arabian Sea, though such incidents are likely to be infrequent and deniable in nature.

A sustained effort to block the Strait of Hormuz remains an unlikely worst-case. Nearly one-fifth of global oil and gas passes through the waterway each day, so any disruption would destabilize energy markets, raise insurance premiums, and increase shipping costs. Such a move would also severely harm Iran's own economy, which relies on the same shipping routes for its exports. A full blockade is therefore unlikely except in a scenario of extreme escalation.

Cargo ship traveling.

Likely Effects of Tariffs, Sanctions, and Grey-Zone Activity

TRADE POLICY SHIFT	SANCTIONS ON ENERGY EXPORTERS	GREY-ZONE MARITIME ACTIVITY
Examples	**Examples**	**Examples**
— US tariffs on Chinese goods — Fees on Chinese-built ships	— US "maximum pressure" sanctions on Iran — Continued restrictions on Russian energy and shipping	— Iranian harassment or tanker seizures — Ukrainian deniable strikes on Russian vessels — Russian shadow fleet
Likely Effects	**Likely Effects**	**Likely Effects**
— Redirects cargo to alternative ports — Congests secondary hubs, lengthens delivery times, and drives volatile freight rates — Raises risks of tariff-evasion practices (ship-to-ship transfers, flag hopping)	— Increases compliance burdens and use of shadow fleets — Raises insurance costs and rerouting needs — Disrupts energy flows and heightens exposure at chokepoints	— Elevates risks in chokepoints (Strait of Hormuz, Black Sea, Baltic Sea) — Heightens threat to shipping and port infrastructure — Prompts rerouting, higher insurance, and delays

Russia's Shadow Fleet and Sanctions Pressure

Efforts to constrain Russia through sanctions – and to pressure Moscow into ending the war in Ukraine – will continue to shape maritime dynamics in 2026. Ukraine is likely to sustain deniable attacks on vessels linked to Russian energy exports and military logistics. Russia's shadow fleet, comprising more than a thousand poorly maintained, under-insured tankers, will remain in service for as long as international sanctions remain in place. This fleet heightens environmental and safety risks, particularly in congested waterways such as the Bosphorus Strait and Baltic Sea, and drives up compliance and insurance costs for legitimate operators. Moscow has also been accused of using shadow-fleet tankers to conduct intelligence gathering and disruptive activities against NATO-linked infrastructure, further elevating security risks in European waters.

Secondary sanctions on countries trading with Russia – notably India's purchase and refining of Russian crude for Western markets – could further disrupt global energy flows. Closing this sanctions loophole would create ripple effects across energy markets and maritime trade, as refiners and shippers absorb significant compliance burdens.

OUTLOOK

Through 2026, the maritime environment will remain unpredictable. Companies will often need to employ creative solutions to economic and operational disruptions that can arise with little warning.

Increasing trade competition will continue to reshape shipping routes and alter port usage patterns, forcing operators to adapt to shifting gateways and volatile costs. US pressure on Iran and Russia will sustain grey-zone activity and raise the risk of a deterioration in maritime security.

This combination of economic pressure and insecurity will keep freight costs elevated, drive up insurance premiums, and heighten the likelihood of disruption across global shipping lanes.

Stronger Responses Required

Operators should plan for regulatory whiplash, rerouted cargo, and shifting port loads. Grey-zone activity and compliance pressures will intermittently stress schedules, insurance, and safety. Flexibility and pre-planned triggers will be essential in 2026.

MITIGATION STRATEGIES

- **Planning:** Embed intelligence-led triggers, flexible contracts, and layered protection into day-to-day planning.
- **Supply Chains:** Secure contracts with two alternative ports and inland routes. Set a 48-hour trigger to switch to backup shipping lines and hold priority stock near end markets.
- **Workforce:** Run ship and terminal safety drills quarterly, and provide crews with guidance on operating in high-risk ports.
- **Financial Planning:** Maintain a financial reserve and automatic route insurance. Budget for higher upfront costs at alternative gateways, emergency power, and strengthened vessel protection.

SIGNALS TO WATCH

- **Tariff Shifts:** New or paused US tariffs and fees on Chinese goods or vessels that could suddenly reshape trade routes and port usage.
- **Iranian Escalation:** Harassment of vessels, tanker seizures, or more severe activity around the Strait of Hormuz, Persian Gulf, or Arabian Sea.
- **Russia/Conflict Spillovers:** Shadow fleet accidents, or tighter secondary sanctions on Russian crude.

RECOMMENDED ACTIONS

Program-Level Actions	Day-to-Day Measures
Embed intelligence-led triggers in planning; bake flexibility and layered protection into operations.	Use a 48-hour trigger to shift to backup shipping lines; hold priority stock near end markets.
Secure contracts with two alternative ports and inland routes; pre-agree conditions to switch lines quickly.	Run ship and terminal safety drills quarterly; brief crews on high-risk ports.
Maintain a financial reserve; ensure automatic route insurance to cover deviations.	Budget for higher upfront costs at alternative gateways, emergency power, and vessel protection.

Southampton docks at dusk.

SUB-SAHARAN AFRICA

EXECUTIVE SUMMARY

Over the coming year, the US shift to a more transactional, security-driven approach, coupled with further scaling back of Western engagement on the continent, will push Sub-Saharan African governments toward longtime players like China and non-traditional partners. In this fluid, multipolar landscape, opportunistic African leaders will exercise greater agency through calculated domestic and cross-border power grabs, often at the expense of traditional governance norms. Changing dynamics will bring near-term commercial opportunities but increase risks of external leverage, political pressure, and social unrest. At the same time, AI-driven disinformation and deepfake-enabled fraud will expand, shaping public sentiment and elevating reputational and financial risk for firms and travelers across the region.

EVENTS TO WATCH

- **Election-season disinformation.** AI-driven rumors will likely spike around 2026 polls in Benin, Uganda, Republic of Congo, Zambia, and South Sudan, raising the likelihood of protests and travel/brand risk.
- **Resource nationalism escalations.** Burkina Faso and Niger are threatening to extend nationalizations or even detain executives. Mali is less defined by stringent resource policy (e.g., Mali/Barrick dispute) than by a worsening jihadist insurgency. However, all three countries represent climates in which businesses will need to be prepared for unfavorable contract renegotiations, asset access limits, and higher exit costs alongside militancy risks.
- **Assab port flashpoint.** Any further push for Ethiopia's access to the Red Sea will trigger tit for tat moves with Eritrea – a dangerous dynamic that, if left unchecked, risks outbreak of more serious fighting that leads to corridor disruptions and spikes in shipping insurance premiums.

KEY JUDGMENTS

The US' transactional approach and reduction in aid expenditure are pushing governments toward China and non-traditional partners, likely raising the risk of destabilization and conflict; operating risks are increasing.

Foreign investment offers short-term relief but will erode governance standards and stability, and increase external pressure to suppress domestic opposition.

Several African governments are exercising greater strategic agency, balancing external suitors to secure capital, technology, and security assistance, even as mounting fragility and insurgent encirclement, particularly across the Sahel, undermine governance and amplify anti-Western sentiment.

AI-generated content on social platforms will expand, reshaping sentiment; actors may exploit it to incite unrest and violence.

Criminal syndicates will escalate deepfake-enabled scams and fraud; businesses and travelers face higher financial and reputational risk.

Industrial dockside cranes illuminated at night in Lobito port.

New Partnerships, Old Dependencies: Africa Navigates a Multipolar Landscape

US aid pullbacks and protectionist trade policies will push Sub-Saharan African governments toward China, Russia and non-traditional partners (Türkiye, Qatar, UAE) throughout 2026. Gulf capital, in particular, is increasingly shaping development finance and infrastructure deals, adding a new pole of influence on the continent. These ties will bring near-term funding but likely erode sovereignty, deepen external leverage, and increase internal conflict risk as new state-led, transactional alliances reinforce dependency and narrow domestic policy autonomy for many African nations.

Severe cuts to US assistance – including dismantling the US Agency for International Development (USAID) and ending the President's Emergency Plan for AIDS Relief (PEPFAR) in 2025 – will likely unravel decades of progress in poverty alleviation, health, food security, governance, and human rights. As France, the UK, Sweden, and Germany also scale back, China, Russia, and others are filling gaps with infrastructure, energy, and security investments that prioritize state control over pluralism. China's state-led model and Russia's support for post-coup juntas will likely suppress civil society in countries like Zambia and Mali, entrench elite capture, and weaken political accountability.

Mid-2025 US tariffs on key African exports (minerals, agricultural goods) will further constrain growth and push states toward alternative partnerships and regional frameworks such as the African Continental Free Trade Area (AfCFTA). These alliances may offer immediate relief but risk again tethering local economies to foreign agendas. In Zambia, Chinese debt restructuring tied to mining concessions has silenced opposition; in Sudan, foreign-backed proxy conflicts have destabilized governance. In 2026, these dynamics will deepen, reinforcing dependency, narrowing policy autonomy, and amplifying social tensions amid a fluid and increasingly multipolar contest.

COMPETING FOR INFLUENCE

The US's shifting strategy will fuel a multipolar scramble for influence in Sub-Saharan Africa in 2026. China, an already major player on the continent, has a head start in any competition with Russia, Türkiye, Qatar, and the UAE – all of whom will continue to try to secure leverage via contracts, capital, and proxies. As traditional Western influence wanes, these powers are pursuing distinct but overlapping strategies that blend commercial, security, and political influence across the continent.

China. Resource-tied loans and China's state-led development model will suppress civil society and align elites with Beijing, fostering economic dependency and stalling reform. The 2024 Forum on China-Africa Cooperation and 2025 Beijing Action Plan commitments point to a 9-percent annual investment growth through 2027, with foreign direct investment (FDI) up by 10 percent in 2026, focused on infrastructure, renewables, and critical minerals (cobalt, lithium). Projects like Nigeria's rail expansions and Congo's green-energy initiatives fill US funding gaps and lead to commercial opportunities. However, foreign-sponsored projects can lead to societal marginalization (e.g., Zambia). China's development model will further expand in Ghana and Angola in 2026, encouraging longer-term dependencies and weakening accountability.

Russia. Security and information operations support will bolster Sahel juntas and destabilize regional power balances. Despite economic constraints, Russia's energy and mineral investments surged in 2025, with FDI projected to grow 17 percent in 2026. In Mali and Burkina Faso, Moscow supplies arms, military contractors, and anti-imperialist narratives; by mid-2026, influence will likely extend to Niger, inflaming ethnic tensions, complicating counter-terrorism operations, and advancing bids for Red Sea naval access.

Türkiye. A commercial-security hybrid will reshape local security architectures as Ankara fills gaps left by the US. 2025 initiatives (Somali port upgrades, oil exploration) marked a 15 percent investment growth, with trade projected to rise by 8 percent and investments by 20 percent through 2027. Turkish trainers are strengthening Somali forces against al-Shabaab, effectively replacing prior US roles. Expanded programs across the Horn may help contain insurgencies, stabilize the local security environment, and create commercial opportunities. Nevertheless, these expanded programs also risk creating regional dependence on Turkish equipment and support, tying fragile states to Ankara's objectives.

UAE. Maritime and conflict-driven investments will tighten control of strategic corridors and fuel proxy dynamics. UAE port projects in Angola, Somaliland, and across the Horn are projected to rise 20 percent in 2026 to secure maritime choke points. Alleged involvement in Sudan's civil war, including arms to the Rapid Support Forces (RSF) per UN reporting, has fractured governance. In Ethiopia, UAE-backed port deals tied to Red Sea ambitions are straining relations with Eritrea, raising the risk of conflict by mid-2026.

Qatar. Targeted investments will reshape East African politics while countering Gulf rivals. Commitments in mining and infrastructure – projected to grow 11 percent through 2030 – include Rwanda's Bugesera Airport. Support for Islamist-leaning groups in Rwanda has contributed to muted opposition, and influence is expected to extend to upcoming elections in Ethiopia and Somalia, potentially tilting outcomes of pro-Qatari factions.

As a by-product of this multipolar competition, a new era of African agency is emerging, with regional powers acting unilaterally to secure their interests amid waning Western oversight and conditionality. From Rwanda's assertive cross-border operations into eastern DRC and Mozambique to Tanzania's tilt toward authoritarianism as the ruling party there seeks to impose its will on the increasingly disillusioned electorate, many African governments are asserting control through repression and military might rather than reform, heightening regional volatility.

CONTEST OVER STRATEGIC ASSETS

Through 2026, competition among global and non-traditional powers for Africa's cobalt, lithium, key ports, and military bases will intensify. While China, Russia, Türkiye, and the Gulf States continue expanding their commercial and security footprints, the US is recalibrating its approach – focusing on targeted infrastructure and critical mineral partnerships to counter Chinese dominance. As rival models of engagement take hold, higher odds of resource-linked conflict and faster environmental degradation are likely, even as new US-backed projects aim to promote supply chain transparency and long-term autonomy.

Minerals (DRC and beyond). China's cobalt lead faces growing competition from the UAE and Türkiye, with UAE mining investments up 20 percent and Turkish energy projects up 15 percent. Intensified extraction will likely heighten local conflict risks and environmental harm.

US alternatives lag. The Lobito Corridor – intended to counter China through mineral deals and trade agreements (including controversial arrangements with nations like Rwanda accepting US deportees for economic concessions) – continues to trail Chinese speed and scale.

Ports, bases, and sea lanes. Russia's planned naval hub in Sudan – backed by a 25-percent increase – and Türkiye's expanding role in Somalia contrast with Washington's efforts to maintain influence through joint maritime patrols and logistics partnerships in Djibouti and Kenya. The UAE's Berbera port project is set to grow 18 percent, and China's Djibouti contracts are up 10 percent, tightening control over Red Sea and Indian Ocean routes.

Aviation footholds. Qatar's stakes in Rwanda's Bugesera Airport and Ethiopia's aviation upgrades – projected to rise by 12 percent – signal bids for regional air dominance.

Red Sea flashpoints. Ethiopia's push for access to Eritrea's Assab port will likely escalate tensions by mid 2026, as Asmara deepens ties with Ethiopia-based armed groups, Egypt, and Saudi Arabia.

Sahrawi refugee camp in Tindouf, Algeria.

THE RISKS OF A FRAGILE CONTINENT

Fiscal austerity, debt servicing pressures, and uneven foreign investments by rival geostrategic competitors – amplified by recent US aid cuts – will strain the region's institutions, fueling unrest, resource disputes, and jihadist threats. Rising civil unrest in East Africa, including Tanzania and Uganda, underscores growing grassroots frustration with inflation, subsidy cuts, corruption, and unmet governance expectations. Expect more protests and service disruptions, higher supply-chain friction, and localized conflict risks as fiscal shortfalls, subsidy cuts, and uneven foreign investment deepen economic hardship and widen security vacuums.

- **Fiscal stress -> unrest.** Budget shortfalls that drove Nigeria's 2025 fuel protests, Kenya's teachers' strikes, and Uganda's hospital shortages will persist in 2026, with subsidy cuts and stalled public sector wages likely to trigger new demonstrations across urban centers. Businesses should expect sporadic demonstrations, labor actions, and service outages in major hubs.
- **Resource disputes.** Tensions over mining rights (Zambia and Congo) and access to Assab port (Ethiopia) will ignite further conflict risk, legal contests, and project delays.
- **Aging infrastructure**. Bottlenecks at critical nodes, such as Kenya's Mombasa port, will increase transport costs and insurance premiums, and delay regional supply chains.
- **Jihadist threats.** Security gaps will empower al-Shabaab in Somalia and Boko Haram/Islamic State West Africa Province (ISWAP) in Nigeria to expand operations, elevating travel and site-security risk in the Horn and Lake Chad regions.
- **Maritime exposure.** Somalia's 2025 piracy surge will raise Red Sea and East Africa-Suez route risk, increasing shipping and insurance costs.
- **Proxy conflicts.** External backing, such as the UAE's involvement in Sudan, will exacerbate grievances and complicate evacuation and overland routing plans.
- **Environmental and governance strain.** Unrest linked to cobalt extraction and governance failures – including corruption and overburdened courts – will undermine local stability and complicate permit access, community-relations and investor confidence.
- **Youth-led protest activity** is likely to increase as younger populations reject aging leaders who they view as no longer representing their values or improving their quality of life.

Africa's 2026 pivot will reshape global markets and geopolitical alignments. Rising demand for critical minerals and Red Sea trade growth will expand the continent's role in global supply chains. Cobalt prices are expected to rise 15-20 percent, and trade volumes in the Horn will approach 1 trillion US dollars. Yet this expansion will expose vulnerabilities: debt sustainability concerns, uneven foreign investment, and policy concessions tied to mineral and trade deals, such as Rwanda's deportee agreement, will test governance and autonomy. If debt traps are avoided, fair trade agreements could lift intra-African trade 15 percent by 2027 (African Union).

A more transactional US approach in 2026 may stabilize near-term partnerships but risks Washington (and other retracting Western countries) ultimately ceding influence to an already influential China, as well as Russia, Türkiye, and the Gulf States. Net result: a more fragmented order will test sovereignty and stability across Sub-Saharan Africa.

Urban aerial view of traffic in Kinshasa, DRC.

AI to Expand Disinformation and Crime in Sub-Saharan Africa

Over the next year, AI-generated content on social platforms will likely expand across Sub-Saharan Africa, shaping political, social, and criminal dynamics. State, party, and activist networks may use these influence campaigns to sway sentiment or incite unrest – especially around elections – while criminals scale deepfake-enabled fraud and scams, creating new risks for businesses and individuals operating in the region.

Election campaign posters in Lagos, Nigeria.

DISINFORMATION CAMPAIGNS IN THE SAHEL AND BEYOND

Sahel pro-Traoré narratives. Pan-Africanist-aligned social accounts are running an extensive campaign supporting Burkina Faso's President Ibrahim Traoré and promoting anti-Western rhetoric. Hundreds of deepfakes and fabricated speeches – surging in May 2025 – cast Traoré as a hero resisting imperialism and foreign exploitation, often comparing him to Thomas Sankara. Despite multiple fact-checks, the content resonates with anger over mineral exploitation and alleged post-colonial interference, sustaining high engagement. Anti-French sentiment in the Sahel and the erosion of Economic Community of West African States (ECOWAS) cohesion (underscored by Mali, Burkina Faso, and Niger's withdrawal from the bloc) will further isolate France and reshape Western engagement strategies.

Business climate effects. AI-generated content is fueling support for Traoré and broader anti-Western sentiment, which could affect how foreign companies operate or expand. In 2025, Burkina Faso, Mali, and Niger nationalized key mineral industries (including gold and uranium) and took hostile actions against firms resisting new terms; Mali even detained Barrick Gold executives amid tax and contract disputes. Such tactics are likely to continue in 2026 as nationalization policies align with public sentiment – particularly against Western companies.

Intercommunal risk. While the current campaign centers on anti-imperialism, its rhetoric could be weaponized to incite unrest or violence against minorities. In the Sahel, Fulani communities are frequently accused of collaborating with jihadists, leading to massacres and targeted violence by security forces and rival groups. Deepfakes featuring popular leaders like Traoré can amplify these narratives and inflame local tensions, raising the risk of renewed clashes.

Election-period manipulation. AI-aided disinformation is also likely during elections or political crises. Campaigns in Côte d'Ivoire during April-May 2025 spread false coup rumors; between May 20-25, posts on Facebook, X, YouTube, and Instagram claimed President Alassane Ouattara had been killed or detained. Some content used AI-generated images; others encouraged coups against governments seen as pro-Western. The wave coincided with Ouattara's plan to seek a controversial fourth term and likely aimed to destabilize his position. Investigations tied initial posts to accounts in Burkina Faso and South Africa before platform-wide amplification.

Engagement and monetization dynamics. These posts drew heavy engagement – some YouTube videos received millions of views and were shared by self-identified pan-Africanist profiles. Like the Traoré deepfakes, they tapped into disillusionment with long-standing leaders linked to Western partners. Financial incentives and follower growth further encourage creators to share unverified content, broadening reach beyond pure political motives.

2026 elections at risk. Benin, Uganda, the Republic of Congo, Zambia, and South Sudan face elevated exposure to similar campaigns. Benin's risk is higher: President Patrice Talon has chosen the Minister of Economy and Finance Romuald Wadagni – educated in the US and France – as his party's candidate, drawing likely opposition from pan-Africanist networks and Traoré supporters. Benin accuses Burkina Faso and Niger of failing to stem jihadist spillover into its north; Traoré accuses Talon of enabling foreign forces. If Wadagni is elected – and especially if another major militant attack occurs in northern Benin – Traoré supporters could launch campaigns to discredit Wadagni and Talon with fake news or claims that they are allowing foreign bases.

EXPANDING CRIMINAL USE OF AI AND DEEPFAKES

Criminal groups are increasingly using deepfakes and accessible AI tools to target businesses, consumers, and governments. Tactics include fake videos, cloned voices, and altered biometric data to defeat onboarding and identity checks.

Where incidents are rising. South Africa recorded a 1,200-percent rise in deepfake manipulation in 2025 (TransUnion). Kenya and Nigeria also saw significant increases over the past year.

Who's most exposed. Financial services and fintech platforms face the greatest risk as fraudsters deploy synthetic identities to open accounts and bypass security controls.

Common schemes. Criminals have filed fraudulent insurance claims, spun up false storefronts, and used AI-generated voices to impersonate bank staff or customers' family members. Deepfake videos of high-profile politicians and public figures are being used to falsely endorse products or services.

Through 2026, AI-enabled fraud and influence tactics will spread across platforms and sectors, blurring lines between political disinformation and criminal schemes. This raises duty-of-care, financial, and reputational risk for organizations and individuals. The priority now is to harden verification, monitor brand misuse, and prepare rapid responses when scams or deepfakes surface. Meanwhile, across the Sahel, jihadist expansion and anti-Western narratives will sustain a security environment too volatile for major long-term projects without state or multi-state guarantees.

RECOMMENDATIONS

- **Awareness and training.** Ensure employees understand current scam patterns and basic info-security; emphasize voice-clone and deepfake risks during verification. AI detection tools can be effective, but best practice remains contacting sources directly for verification.
- **Monitoring and response.** Stand up online threat monitoring and crisis-communications playbooks to spot and address reputational attacks using your brand or executives' images.
- **Exposure is broad.** Assume criminals will target indiscriminately, putting both local and international businesses – and their employees – at risk.
- **Trusted intelligence.** Maintain access to reliable reporting on active disinformation/fraud campaigns to prepare contingency plans before narratives translate into physical threats.
- **Elections and unrest.** Expect AI-enabled disinformation to spike during political tension (corruption, insecurity, foreign interference, anti-imperialism), raising unrest risk.
- **Sahel exposure management.** Limit activity to short-duration projects under explicit government or international mission security coordination; establish redundant evacuation and communication protocols across borders.

SOUTH AFRICA SAW A **+1200% INCREASE IN AI FRAUD** IN 2025
(TRANSUNION)

Young Africans gather at rally in support of Burkina Faso's President Ibrahim Traoré, who benefited from hundreds of deepfakes casting him as a hero resisting imperialism.

GLOBAL HEALTH

Medical helicopter landing.

GLOBAL HEALTH

MISINFORMATION AND DISINFORMATION POSE A SIGNIFICANT THREAT TO GLOBAL HEALTH

EXECUTIVE SUMMARY

Health-related misinformation and disinformation will remain one of the most pressing challenges to global health security. False narratives – particularly around vaccines – undermine trust in institutions, weaken immunization programs, and erode pandemic preparedness. Social media platforms and generative AI amplify these risks by enabling the rapid creation and spread of misleading content, often overshadowing credible guidance. As new infectious diseases and pandemic threats persist, tackling the circulation of misinformation will be central to safeguarding public health. Without stronger interventions, health systems will face reduced trust, widening inequities, and repeated setbacks in outbreak response.

Monitoring emerging narratives and preparing tailored response strategies – through internal messaging, traveler advisories, or crisis plans – will be critical to protecting employees and sustaining operations in future health emergencies.

KEY JUDGMENTS

False and misleading health information will continue to undermine public trust, fueling systemic vulnerabilities.

Vaccine hesitancy, sustained by false narratives, will contribute to stagnant or declining immunization coverage and recurring outbreaks of preventable diseases.

Organizations that invest in transparent communication, evidence-based policies, and partnerships with trusted providers will be better positioned to manage misinformation risks.

Pandemic preparedness will weaken as eroded trust undermines compliance with emergency measures and slows rapid response.

Two researchers working in medical laboratory.

Threat Landscape

MISINFORMATION AND DISINFORMATION

Health-related misinformation and disinformation will continue to threaten global health systems. Misinformation refers to false information shared without intent to deceive; disinformation is deliberately false and spread to cause harm. Left unchecked, both will undermine decision-making, weaken health systems, and erode trust.

TECHNOLOGY AMPLIFIERS

The spread of false information is likely to grow as social media remains a primary source of information. Algorithms create echo chambers that reinforce existing beliefs, while generative AI can produce convincing synthetic content that blurs fact and fiction. Together, these dynamics will overwhelm credible sources, weaken public health campaigns, and shape perceptions that entrench misinformation.

LASTING IMPACT OF COVID-19

The pandemic showed how quickly false narratives can overwhelm credible sources. Conspiracy theories about COVID-19's origins and false claims about vaccine safety spread faster than official guidance, often overshadowing scientific advice. The resulting oversaturation of conflicting information eroded trust in health institutions, complicated response efforts, and left lasting doubts about health policies and science. These dynamics will likely recur in future crises, making outbreak management and public compliance more difficult.

CONSEQUENCES FOR PUBLIC HEALTH

If misinformation remains unchecked, trust in health authorities and scientific institutions will decline. This erosion of confidence fuels resistance to public health measures and politicizes health decisions, destabilizing communities and complicating emergency responses. Reduced trust leads to vaccine refusal, reliance on alternative medicine, and disregard for professional guidance. Once lost, confidence is slow to restore, leaving societies less prepared to manage future health threats.

VACCINE HESITANCY

Misinformation will fuel vaccine hesitancy, contributing to the resurgence of preventable diseases such as measles, pertussis, and polio. Vaccine hesitancy is shaped by the "3 Cs":

- Complacency: a false sense of security from past immunization success.
- Confidence: trust in vaccines and institutions, often undermined by misinformation.
- Convenience: barriers such as access, affordability, and clear communication.

Global immunization programs, already disrupted by the pandemic, will struggle to recover as hesitancy spreads. In 2024, over 14 million children worldwide were estimated to have missed their first dose of diphtheria, tetanus, and pertussis vaccine (DTP1) by the end of their first year of life, leaving significant immunity gaps, especially in fragile states. Major measles outbreaks in 2023 and 2025 – including setbacks in regions that had previously controlled the disease – highlight the consequences of stagnant or declining vaccine uptake. Eroded trust amplifies concerns about safety and side effects, exposing vulnerable populations and threatening herd immunity. Vaccine hesitancy fueled by misinformation will remain a significant obstacle to global health security.

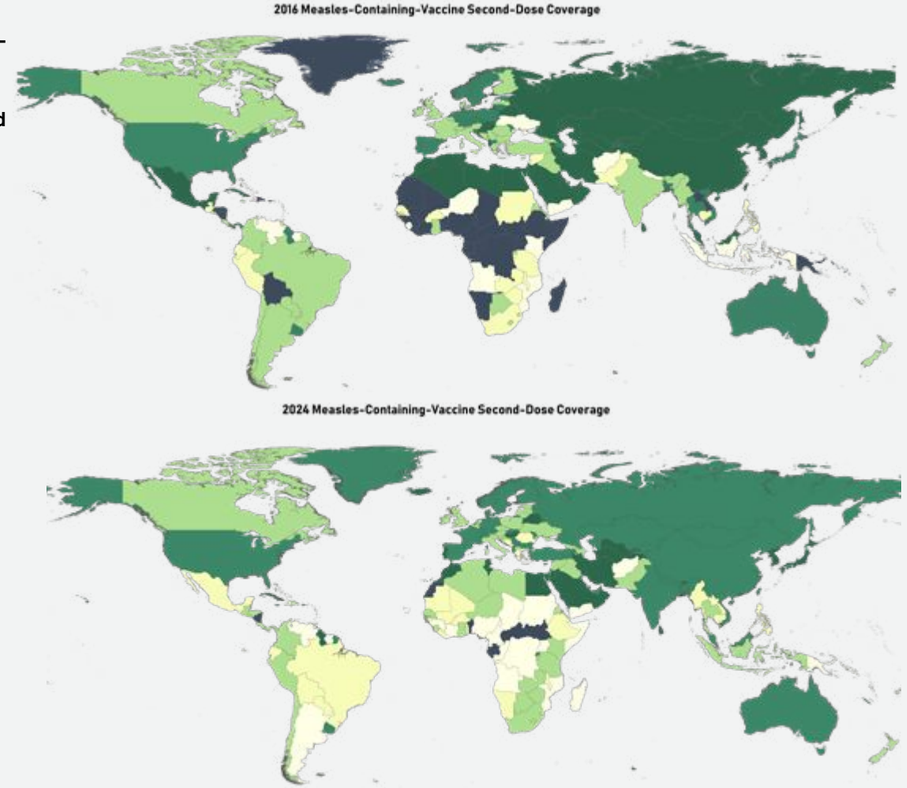
SYSTEMIC STRAIN

Health systems will face mounting pressure as preventable outbreaks increase hospitalizations. Surges in vaccine-preventable diseases will divert resources, worsen staff shortages, and weaken emergency response capacity. If misinformation continues to drive vaccine refusal, these strains will become recurring features of public health planning.

Existing inequities are expected to deepen as communities with limited access to healthcare and reliable information will remain vulnerable to misinformation and its consequences. Global immunization coverage has stalled, and without renewed momentum, under-vaccination will persist in low- and middle-income countries. These gaps risk fragmenting global health security and weakening collective immunity.

WHO/UNICEF Estimates of Measles-Containing-Vaccine Second-Dose Coverage for 2016 and 2024

The map shows the percentage of children who have received two doses of measles containing vaccine (MCV2) in a given year (2016 vs 2024), by country, according to the nationally recommended schedule. This is based on WHO/UNICEF Estimates of National Immunization Coverage (WUENIC).



REFINED PREPAREDNESS RISKS

Misinformation will undermine compliance with emergency measures in future pandemics. Resistance to vaccination and protective guidance could delay containment, prolong outbreaks, and increase health and economic costs. Even after COVID-19, disinformation may continue to erode public cooperation, strain health systems, and expose gaps in preparedness. Future campaigns will likely exploit uncertainty, making rapid and effective response more difficult for governments and health authorities.

OUTLOOK

Misinformation and disinformation will continue to undermine vaccination efforts, strain health systems, and weaken global preparedness for pandemics. Without coordinated interventions, societies risk recurring outbreaks, deeper inequities, and longer recovery from health crises. Organizations that invest in transparent communication, evidence-based policies, and partnerships with trusted providers will be better positioned to manage misinformation risks. Monitoring emerging narratives and preparing tailored response strategies – through internal messaging, traveler advisories, or crisis plans – will be critical to protecting employees and sustaining operations in future health emergencies.

SIGNALS TO WATCH

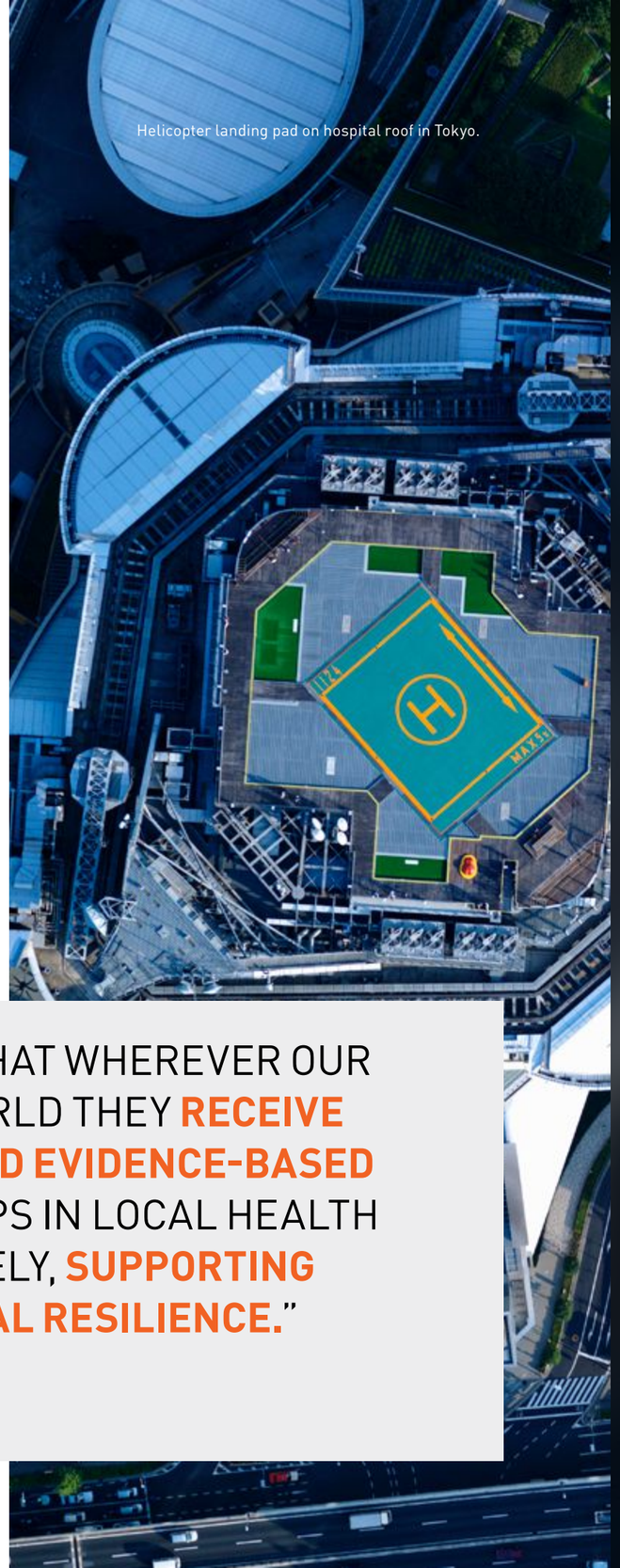
- → **Vaccine uptake trends:** where coverage stalls or declines, signaling heightened vulnerability.
- → **New disinformation tactics:** especially the use of AI to amplify narratives.
- → **Public trust in health institutions:** levels of confidence shaping compliance with future emergency measures.

GLOBAL HEALTH

Global Health Security: Ensuring Consistent Standards of Medical Care Across Borders

In this Q&A, Crisis24 Medical Director Craig Stark, MD, FACP, explains how the company's medical governance model ensures evidence-based consistency across global healthcare systems.

CRAIG STARK, MD, FACP
MEDICAL DIRECTOR
Crisis24



Helicopter landing pad on hospital roof in Tokyo.

"OUR MODEL ENSURES THAT WHEREVER OUR CLIENTS ARE IN THE WORLD THEY **RECEIVE CLEAR, CONSISTENT, AND EVIDENCE-BASED CARE.** THIS BRIDGES GAPS IN LOCAL HEALTH SYSTEMS AND, ULTIMATELY, **SUPPORTING GLOBAL ORGANIZATIONAL RESILIENCE.**"

- CRAIG STARK, MEDICAL DIRECTOR, CRISIS24

Q: Healthcare standards can vary significantly across different countries and regions. How can clients receive reliable medical guidance and coordinated care regardless of where they are in the world?

A: Our clients operate globally, so care has to work in the real world. At Crisis24, our doctors and nurses start by looking at each case in its local context – what resources are available, what the standard pathways are, and where there may be gaps. From there, we recommend practical upgrades that align with international guidelines and well-established clinical practice.

Within our Global Operations Centers (GOCs), medical professionals work closely with operations and security teams to ensure that clinical insights translate into timely and coordinated action. This integrated model allows information to move quickly across regions and time zones, ensuring that decisions are based on consistent medical reasoning rather than regional variability.

Q: Many developing nations face resource constraints. What challenges do you encounter when working in emerging-market countries with limited healthcare resources?

A: In many emerging-market countries, healthcare decisions are shaped by public health priorities. Conservation of assets and the greater good of the broader population can at times take precedence over what is optimal for the individual patient.

Limited healthcare resources often mean our clinicians must make complex decisions within real constraints – whether that's a lack of diagnostics, restricted medication supplies, or limited specialist access. For our clients, that can translate into longer wait times, fewer treatment options, or the need to travel long distances for care. In these situations, our teams work closely with local providers on behalf of our clients to ensure they receive the care they need, including referrals to higher-level facilities, additional diagnostics, or revised treatment plans to meet global benchmarks.

Q: Can you share a specific example of how this medical oversight works in practice?

A: We manage a wide range of cases, from urgent interventions to the more complex, extended care coordination, and the process is the same: assess locally, compare to current guidelines, and then coordinate the right next step. In one recent case, a traveler sustained a dog bite in a rural area and was treated at a local clinic with antibiotics, a rabies vaccine, and wound cleaning – but not rabies immunoglobulin (RIG). Our GOC medical team reviewed the case, and determined the plan did not meet international standards for rabies post-exposure care. The team coordinated with local providers and arranged for the traveler to move to a nearby country where both the vaccine and RIG were available. The intervention ensured the traveler received appropriate, potentially life-saving care and demonstrated how our medical oversight can bridge gaps in local health capacity and capability.

In another case, a university faculty member in Addis Ababa, Ethiopia, developed pneumonia with complications that required intensive monitoring. Our medical team evaluated the capabilities of the local hospital and concluded they had the right level of expertise to treat him safely. We maintained daily contact with the treating team for nearly two weeks, making sure his treatment and progress was on track. Once he was stable enough to travel, we organized his flight home with medical support and oxygen on board, and ensured he made it home safely to the US and into the care of his primary healthcare provider.

These examples show how medical oversight turns clinical judgment into action – closing gaps, avoiding unnecessary transfers, and moving quickly when escalation is needed.

Q: Beyond intervention, what measures can travelers take to prevent medical issues while abroad?

A: Preparation is the best prevention. At Crisis24, pre-travel medical guidance is a core part of our care model. Before clients travel, our medical teams use the latest intelligence to anticipate health risks travelers may face – whether that's a local disease outbreak, extreme climate conditions, or region-specific safety concerns.

We help clients understand those risks and take practical steps to protect themselves, such as reviewing vaccinations against current international guidance, arranging required immunizations and documentation, and sharing advice on hydration, food safety, and insect-borne disease prevention. This proactive approach helps travelers stay healthy and confident, wherever they're headed.

Q: What broader impact does this approach have beyond individual patient care? How does it affect organizations?

A: Providing clear and consistent medical advice reinforces confidence in an organization's ability to manage risk responsibly. In an environment where misinformation and uneven care standards can cause confusion and put people at risk, a proactive approach to medical assistance supports global organizational resilience.

THE EXPERTS' TAKE

Two workers consult laptop in lobby.

AI and Security: Reimagining Global Risk Management

In this Q&A, Crisis24's Cathy Gill, Vice President, Product Management, and Chris Hurst, Vice President, AI and Innovation, discuss how AI can enhance security's ongoing evolution toward more proactive, anticipatory operations. In this way, organizations are empowered to move faster, communicate more clearly, and recover with greater confidence.

CATHY GILL
VICE PRESIDENT,
PRODUCT MANAGEMENT
Crisis24

CHRIS HURST
VICE PRESIDENT,
AI AND INNOVATION
Crisis24

Aerial view of Earth from space.

Q: How is AI reshaping the way security and resilience teams operate, and what makes it such a powerful force multiplier in risk management?

CH: The nature of risk itself has changed – again. From surveys over the last 12 months, our industry data shows nearly two-thirds of security leaders believe we have entered a new post-COVID inflection point. From uncertainty about tariffs and global trade to rising geo-political tensions (Iran-Israel, Russia-Ukraine, China-Taiwan) to continued extremes in natural disasters (e.g., LA fires), security and risk professionals are being asked to respond strategically and tactically like never before. And of course, dynamic risks continue – where threats evolve or escalate mid-crisis and produce cascading impacts that extend beyond what's expected.

There is also greater expectation for security teams to manage complex scenarios at greater speeds and with increasingly sophisticated and nuanced responses at every stage of an event's impact. Within the strategic uncertainty, security teams must continue to handle multiple, interconnected consequences – such as a tornado touchdown leading to a gas main break, road closures, evacuations, and workforce disruptions. Each event requires different standard operating procedures that must seamlessly integrate to provide executives with clear situational understanding and employees with consistent communication and assistance.

Here is where AI is front and center as the next generation of resilience management. It can streamline workflows with continuous monitoring, insightful summaries, and timely updates. AI accelerates threat detection and analysis, drafts communications, handles routine tasks, tracks assets, and surfaces insights – keeping security teams aligned and enabling personnel to focus on critical decisions. While AI increases coverage, efficiencies, and capacity for larger global operations centers (GOCs), it's with smaller or single-person teams where it becomes a real force multiplier, expanding limited resources exponentially.

Q: Are humans still central to intelligence analysis and threat assessments, even when augmented with AI? How can leaders strike the right balance between automation for speed and oversight for judgment and compliance?

CG: Absolutely. Humans remain central because AI, while powerful at processing data and identifying patterns, still has gaps in contextual understanding, ethical reasoning, and nuanced judgment that security operations demand. At Crisis24, our AI-powered monitoring systems detect approximately 20,000 candidate incidents daily, but human analysts are essential for interpreting cultural and political context, understanding regional nuances, and making judgment calls that could affect lives and livelihoods. AI can tell us what happened; analysts are still needed to reliably determine what it truly means and what we should do about it.

CH: The key to balancing automation with human oversight lies in designing complementary workflows where each handle what they do best. We want our analysts operating at the "top of their license," so we automate data collection, initial threat detection, pattern recognition, and routine communications to free up human analysts for high-value decision-making. This framework ensures humans remain in control at critical decision points: validating AI outputs before they reach clients, interpreting ambiguous or unprecedented situations, and maintaining accountability for security recommendations. AI excels at the "what" and "when," while humans provide the "why" and own the decision of what action to take.

CG: We implement multiple checkpoints throughout our processes to maintain this balance. Technical safeguards prevent AI from making autonomous decisions, while human analysts maintain oversight through continuous monitoring, regular model validation, and exception handling. When AI flags something as a potential incident or threat, a human analyst reviews the context, assesses the credibility, and determines the appropriate response. This approach maximizes the benefits from the speed that AI provides and the judgment that human expertise can deliver, ensuring compliance and veracity while maintaining the agility that modern security demands.

Q: How do the AI-powered features in Crisis24 Horizon enhance and strengthen critical event management and crisis communication?

CG: Horizon is a unified platform that helps clients cut through the noise, compressing the time between detecting a threat and taking action. The new "Ask Horizon" assistant brings conversational AI into both proactive risk management and crisis response. Want to see who may be impacted by the earthquake in Thailand or assess the risk of terrorism in Algeria for upcoming business travel? Want Horizon to compose a message to at-risk personnel during a hurricane for every messaging modality? Just Ask – and then act!

Another tool is Horizon's Latest Event Synopsis. It takes all the latest alerts in a location and provides a concise, AI-generated summary in one brief. Instead of reading through all the alerts individually, you have a clear, rapid understanding of what's happening on the ground.

AI and Security: Reimagining Global Risk Management

This is powered by our AI-augmented intelligence that continuously monitors global events and provides greater visibility into what's happening around the world in relation to a client's assets and operations. And this represents just the beginning of our AI integration. We have significant additional capabilities under development that will further transform how organizations manage risk and increase resilience.

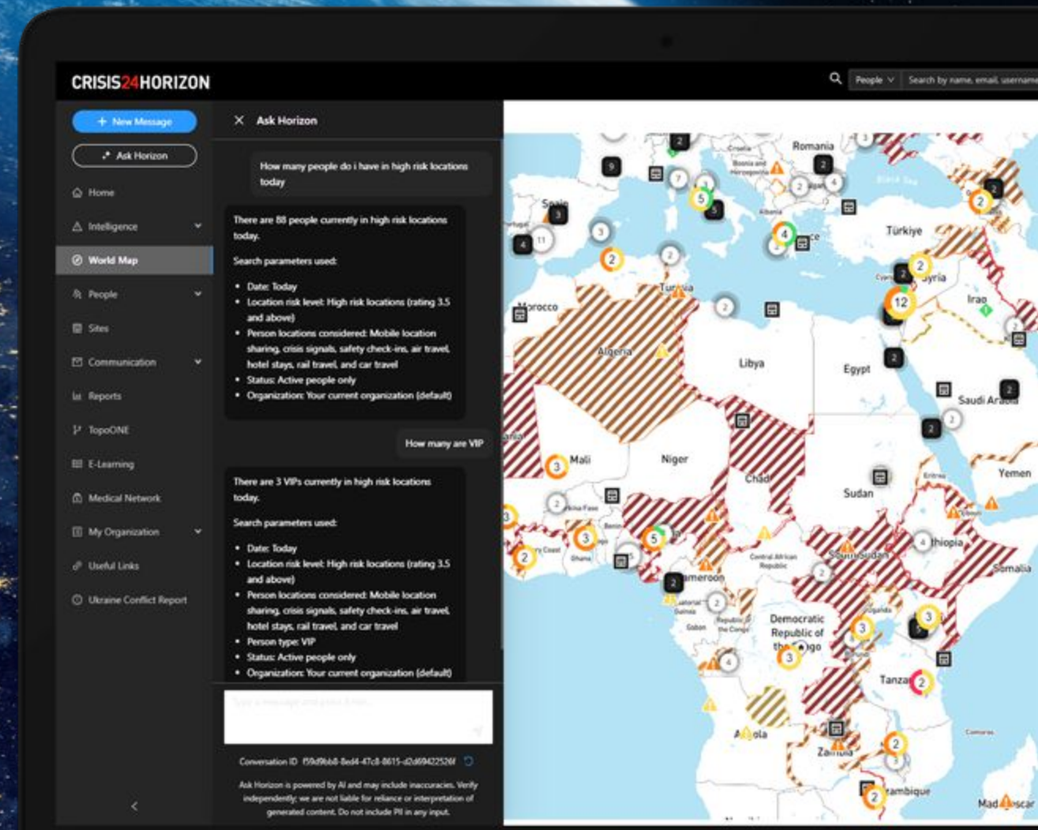
Q: Looking ahead, how will responsible AI redefine resilience for organizations navigating complex global risks?

CH: We're moving toward a fundamentally different paradigm for organizational resilience, manifested in three areas. First, responsible AI will enable predictive risk modeling that anticipates vulnerabilities before they manifest. Instead of reactive crisis management, organizations will have continuous risk intelligence that adapts in real-time to changing conditions, emerging threats, and evolving operational contexts. This represents a shift from managing individual incidents to orchestrating comprehensive resilience strategies. Second, AI is increasingly strong at understanding context. Of course, this only works when the models are given and trained on the appropriate context. But when they do, they can help focus impacts and actions to the user, improving actionability. Finally, we expect to see adoption curves in our industry that enable true scale – from "agentic assistants" to "human-agent teams" to "human-led, agent orchestrated" – with "human in the loop" (HITL) and "human on the loop" (HOTL) firmly in place for critical decisions.

CG: This requires responsible AI development that prioritizes transparency, accountability, and human agency, with clear audit trails and human oversight. The goal isn't to replace human decision-making but to provide managers with unprecedented situational awareness and strategic options, enabling them to navigate complexity with confidence and advance their security operations toward even more anticipatory and proactive capabilities.

WHAT IS CRISIS24 HORIZON?

Horizon is a unified risk management platform, built on a modern technology stack to provide organizations with unprecedented access to dynamic and intrinsic intelligence, travel/people/sites risk management, mass notification, and critical event management.



Aerial view of Earth from space.

THE EXPERTS' TAKE

Navigating Tomorrow's Cyber Threats: AI, Layered Security, and Proactive Defense

Crisis24 cybersecurity experts Ghonche Alavi, Director of Cybersecurity, and Ante Batović, PhD, Senior Consultant, explore how organizations can build comprehensive defenses against an evolving threat landscape where digital and physical risks increasingly converge.

GHONCHE ALAVI
DIRECTOR OF CYBERSECURITY
Crisis24

ANTE BATOVIĆ, PHD
SENIOR CONSULTANT
Crisis24

Businessman reading tablet.

Q: How has AI transformed the cyber threat landscape, and what should organizations prepare for in 2026 and beyond?

AB: AI has fundamentally changed how threat actors operate and increasingly functions as a powerful enabler for threats we've seen before – such as ransomware, impersonation, business email compromise, and supply chain attacks. With AI, malicious actors can automate and scale campaigns quite efficiently, making sophisticated attacks easier to perpetrate.

GA: AI's impact is not just about volume, but also verification. Previously, training focused on spotting grammatical errors or inconsistencies in phishing attempts, but AI has eliminated many of those tells. Now, even voice and video can be convincingly impersonated, making it much harder to verify identities. For example, family offices are concerned about two-factor authentication for large transfers. If a voice call can be convincingly faked, traditional verification methods are undermined. The threat landscape is now a constant game of cat and mouse, and we have to adapt our cybersecurity tactics accordingly.

Q: What are the most common blind spots organizations and individuals have when it comes to protecting their digital security?

AB: Over-reliance on technology and neglecting organizational culture are major blind spots. Many organizations don't think they need cyber insurance, even with daily news of attacks. Supply chain vulnerabilities are also critical; companies often lack visibility into the cyber resilience of their vendors, which can be exploited as entry points.

GA: Sometimes organizations have cyber insurance and assume that's enough, without testing their plans or knowing their vendors. On the family side, there can be an assumption that children's digital footprints are limited, but exposure through schools, clubs, and other organizations reveals sensitive schedules and data. The blind spot is not considering all the actors and organizations connected to your data. Insider threats are another gap, and most organizations don't monitor them proactively and often investigate only after an incident occurs.

Q: How does Crisis24's integrated approach differ from traditional cybersecurity providers?

GA: Our approach is holistic – we don't just look at the technical side, the "ones and zeros." We integrate physical security, information security, and digital footprint analysis. Most providers conduct assessments in silos, but we combine these perspectives. Simulated pen testing is just a snapshot in time; we focus on structure, governance, and enterprise risk management, ensuring cyber fits into the broader risk picture.

AB: Insider threats are also a major risk, and most organizations lack proactive approaches to detect them. Our insider threat programs leverage AI to analyze behaviors and patterns across large populations – not just IT and cyber but also other risk pillars. It's an integrated, context-driven approach that allows us to adapt solutions to any organization's needs, whether they're defense organizations concerned about sabotage or crypto enterprises trying to manage complex custody chains.

Q: How should organizations respond to the surge in crypto crime, and what makes certain targets more vulnerable?

GA: We distinguish between mature financial institutions, which typically have strong governance and robust verification processes, and individuals who may lack discretion and are therefore more exposed. Those who discuss their holdings publicly – on podcasts or social media, for example – can become prime targets quickly.

AB: Public exposure can make executives and their families targets, so we provide training and recommendations on digital footprint reduction, asset storage, and personal security to help reduce risk. Vulnerabilities are created in many ways – for example, if someone's LinkedIn profile shows they're a crypto executive, if property records reveal addresses, or if social media exposes family routines. Therefore, extra vigilance is certainly warranted.

Q: What does "layered security" mean in practice, and what lessons from recent high-profile attacks should shape the way organizations think about resilience?

GA: Layered security means combining multiple defenses, such as executive protection, privacy programs, and digital footprint management. This matters because threat actors will always look for the weakest link. Every connection, whether to organizations, vendors, or family members, widens the attack surface. It's not a single point of entry; comprehensive protection is required. Recent UK attacks, including the Jaguar Land Rover (JLR) incident, show that even large organizations can be crippled if they're unprepared.

AB: Threat actors are opportunists, and they will target low-hanging fruit. Layered security makes it much harder for them to succeed, reducing the likelihood of attack. The JLR attack demonstrates how unsophisticated actors using ransomware-as-a-service can inflict massive damage.

Navigating Tomorrow's Cyber Threats: AI, Layered Security, and Proactive Defense

Preparedness is key; it's not if, but when an attack will happen. Well-prepared organizations lose less money and suffer less reputational damage, and individuals without awareness or strong cyber provisions can face financial, reputational, and even physical risks.

GA: Our philosophy at Crisis24 is to have a plan, test the plan, and test it again. Run tabletop exercises, simulate attacks, and validate vendor relationships. Organizations that treat security as continuous adaptation rather than periodic assessment show better resilience. Whether protecting a multinational or a family office, success requires understanding your context, identifying critical assets, and implementing appropriate controls. In today's environment, standing still means falling behind.

"**OUR APPROACH IS HOLISTIC**. WE DON'T JUST LOOK AT THE TECHNICAL SIDE; **WE FOCUS ON STRUCTURE, GOVERNANCE, AND ENTERPRISE RISK MANAGEMENT**, ENSURING CYBER FITS INTO THE BROADER RISK PICTURE."

- GHONCHE ALAVI, DIRECTOR OF CYBERSECURITY, CRISIS24

Businessman reading tablet.

THE EXPERTS' TAKE

Redefining Intelligence for the C-Suite and Boards

In this Q&A, Geoffrey Hills, Managing Director, and Ansel Stein, Vice President, Operations, of Crisis24 AiiA Powered by Palantir, discuss the origins of AiiA – a game-changing intelligence offering built to give top business leaders defensible foresight and enable faster, better decisions.

GEOFFREY HILLS
MANAGING DIRECTOR
Crisis24 AiiA Powered by Palantir

ANSEL STEIN
VICE PRESIDENT, OPERATIONS
Crisis24 AiiA Powered by Palantir

Moscow International Business Center.

Q: What was the inspiration for Crisis24 AiiA and how does it differ from traditional intelligence products?

GH: The inspiration came directly from our work with some of the world's most respected organizations and recognizable brands. We observed a gap in how decision-makers at the highest levels access and act on intelligence. Tactical insights are absolutely essential for crisis management, but they fall short of delivering the strategic clarity required to lead a global organization effectively. We kept coming back to this question: why do heads of state receive intelligence tailored to support consequential decisions, while C-level and board leaders must navigate unfiltered noise?

AiiA was designed to close this gap by isolating and prioritizing what matters for each organization, synthesizing the data into an easily digestible format, and putting it directly into the hands of top leadership so they can make informed decisions with confidence. It is a groundbreaking approach that heralds a new era in business management where strategic intelligence drives competitive advantage. We leveraged our decades of global risk intelligence expertise and partnered with Palantir, whose platform combines secure data integration, AI infrastructure, and the ability to deploy machine learning and large language models, to power intelligence at this scale.

AS: In practice, AiiA brings together operational, financial, and legal perspectives into a unified enterprise decision framework. It empowers C-level executives and leadership teams who must frequently decide and defend a course of action – whether that's preparing briefings on global risk trends, monitoring geopolitical instability, planning for supply chain resilience, commodities forecasting, or maintaining situational awareness across multinational operations. Where other tools bury the lead in mountains of irrelevant data, we help them spot the opportunities often hidden within the global risk landscape and move quickly to seize them.

Q: How does AiiA transform all of the diverse data sources into strategic clarity?

AS: AiiA pulls in structured and unstructured data from public sources worldwide and applies AI to surface concise, strategic insights. Organizations can see threats clearly, model what's likely to happen and what the consequences might be, and understand patterns in the specific locations or markets that matter most to them. Boards aren't interested in another risk report; they want to know if the organization is resilient and competitive. AiiA connects the dots and provides context specific to the organization's priorities.

GH: This becomes particularly powerful for organizations operating across global markets that extend beyond their in-house regional expertise. The AI does the heavy lifting of filtering out what isn't relevant and highlighting what is, and everything is backed by verified sources. That transparency means the intelligence holds up when you're presenting to boards; in essence, it's enabling fast, defensible decisions.

Q: How does AiiA fundamentally change the way boards and C-level leaders approach risk and opportunity?

GH: AiiA shifts the conversation from reactive risk management to proactive opportunity identification. It helps C-level leaders think with foresight, not hindsight, whether identifying market gaps, evaluating regulatory changes that create advantages, or isolating disruptions that present investment opportunities before they become obvious to competitors. It's about transforming the mindset from "What happened?" to "What's emerging that we can act on right now?"

AS: That shift is critical because boards are constantly being challenged on whether the organization can move fast enough and stay resilient in volatile, uncertain conditions. Risk and opportunity change from moment to moment, and executives must frequently make decisions with imperfect information. AiiA serves as a strategic partner by structuring those imperfect global inputs into executive-ready outputs. No one's time is wasted creating decks or packaging reports.

Q: The President's Brief is the flagship product and first offering from AiiA. How is it structured to deliver maximum value?

AS: Every morning, C-level executives receive an AI-generated briefing tailored to their organization's priorities in a format modeled after intelligence briefings provided to heads-of-state. There's a summary for quick scanning, a concise set of intelligence notes in both short and long versions, complete source citations, and AI-generated commentary that answers the critical "so what" question. It helps executives understand what's happening, why it matters to their organization, and what they should do about it.

GH: The daily cadence provides fresh intelligence every morning, rather than weekly or monthly reports that become outdated by the time they reach the boardroom. The customization runs deep through our Intelligence Priority Framework, built from each client's public corporate documents. We tailor intelligence to individual C-level roles, so the Chief Financial Officer receives different prioritized insights than the Chief Supply Chain Officer. While the content is AI-generated, it's highly personalized and strategically relevant.

Redefining Intelligence for the C-Suite: Crisis24 AiiA Powered by Palantir

AS: Everything is built on trust-by-design. Every insight is auditable with complete source citations and provenance. Proprietary client data is not ingested - we use only public sources, ensuring sensitive information is protected. Onboarding is fast, yet the output meets the sophistication C-level executives and boards expect.

Q: What does the launch of The President's Brief signal about the future of intelligence and risk management at Crisis24?

AS: This launch underscores Crisis24's role as a leader in the future of risk management. For years we've supported organizations at the operational level – helping teams maintain situational awareness, manage crises, and keep people and assets safe. With AiiA, we're extending that same expertise to the boardroom and the C-suite, giving leaders the foresight and defensible intelligence they need to anticipate change and make confident, high-stakes decisions. The President's Brief is just the beginning.

GH: The partnership with Palantir solidifies the AI infrastructure, while our expertise in intelligence selection, integration, and operational oversight ensures the platform evolves with best practices. Our roadmap expands capabilities for global supply chain monitoring and commodity risk analysis, with emphasis on sectors like food and critical infrastructure, plus advanced features such as live analyst access for premium clients. We're redefining what executive intelligence looks like by enabling C-level executives to anticipate change –not merely respond to it – and actually shape the outcome for their organization.

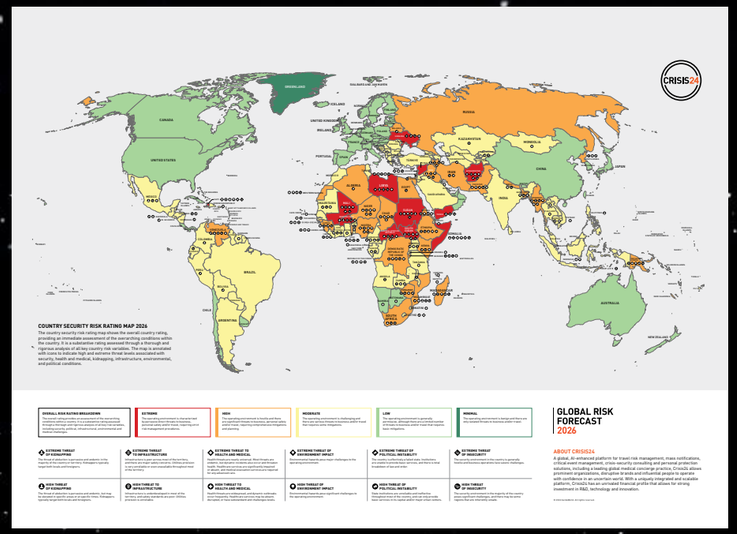
> "AIIA REDEFINES WHAT EXECUTIVE INTELLIGENCE LOOKS LIKE BY **ENABLING C-LEVEL EXECUTIVES TO ANTICIPATE** CHANGE – NOT MERELY RESPOND TO IT – AND ACTUALLY **SHAPE THE OUTCOME FOR THEIR ORGANIZATION**. "
>
> - GEOFFREY HILLS, MANAGING DIRECTOR, AIIA POWERED BY PALANTIR

Moscow International Business Center.

AiiA President's Brief

Risk Assessment Ratings Maps

Crisis24's country-specific security and risk rating maps provide informed indicators of security conditions for a high-level understanding of a country's threat profile. With the assurance of extensive analytical coverage and pressure-tested methodologies, Crisis24 continuously monitors the operating environment and updates threat ratings as conditions change. Each country is rated on a scale from 1–5 (minimal, low, moderate, high, or extreme) to indicate the threat level. The country security and risk ratings provide a clear picture of potential concerns and can help inform risk mitigation strategies.



Included in the 2026 Global Risk Forecast are eight risk assessment maps, consisting of an overall security and risk rating map, specialized category maps, and a master map that reflects the overall country rating with high and/or severe specialized threats specific to each country.

DOWNLOAD MAPS
https://bit.ly/GRF26maps

To access these maps, please visit our digital version by scanning the QR code or typing the address into the browser.

Aerial view of Earth from space.

Contributors

Crisis24 would like to thank our contributors, whose expertise gained from experience in both government and private sector intelligence agencies underpins our support capabilities to our clients, giving us unrivaled depth in the field.

Steven Adam
Intelligence Analyst, Americas

Ghonche Alavi
Director, Cybersecurity

Sharanya Anguraj
Regional Manager, Asia-Pacific

Michael Baney
Regional Manager, Americas

Ante Batovic, PhD
Senior Consultant, Information Security

Jacopo Di Bella
Intelligence Analyst, Asia-Pacific

Terry Berna
Intelligence Analyst, Africa

Barend Botes
Watch Operations Manager

Melissa Chia
Intelligence Analyst, Asia-Pacific

Chris Clough
Intelligence Analyst, Europe & Central Asia

Christian Contro
Intelligence Analyst, Europe & Central Asia

Joe Dvorak
Regional Manager, Europe & Central Asia

Dyna Faid
Intelligence Analyst, Middle East & North Africa

Mawande Gidimisana
GIS Analyst

Cathy Gill
Vice President, Product Management

Larry Henderson
Director, Global Intelligence

Nick Hill
Director, Intelligence

Geoffrey Hills
Managing Director, AiiA Powered by Palantir

Charles Hogger
Intelligence Analyst, Environment

Chris Hurst
Vice President, AI & Innovation

Janna Hyland
Intelligence Analyst, Aviation

Jonathon Keymer
Director, Global Intelligence

Genevieve Labuschagne
Intelligence Analyst, Asia-Pacific

Maria Leasure
Category Intelligence Manager

Grace Lim
Intelligence Analyst, Asia-Pacific

Sally Llewellyn
Vice President, Global Intelligence

Danielle Marais
Intelligence Analyst, Transportation

Robyn Mazriel
Health Intelligence Analyst

Sara Melchiades
Intelligence Analyst, Americas

Brian Moser
Intelligence Analyst, Europe & Central Asia

Adam Prusakowski
Intelligence Analyst, Middle East & North Africa

Daniel Saenz
Intelligence Analyst, Americas

Mick Sharp
Senior Vice President, Operations & Intelligence

Craig Stark, MD, FACP
Medical Director

Ansel Stein
Vice President of Operations, AiiA Powered by Palantir

Allo Tedla
Intelligence Analyst, Africa

Jonathan Vincent
Cyber Intelligence Lead

Tumi Wallace
Regional Manager, Europe & Central Asia

Alex Watt
Intelligence Analyst, Maritime

Tim Williams
GIS Analyst

About Crisis24

Crisis24, a global, AI-enhanced provider of travel risk management, mass communications, critical event management, crisis-security consulting, personal protection solutions and global medical concierge capabilities, allows prominent organizations, disruptive brands and influential people to operate with confidence in an uncertain world. Backed by proprietary AI-enabled SaaS technologies, advanced Global Operations Centers, and the largest team of private sector intelligence analysts in the world, we deliver localized insights and global perspectives alongside medical, security, crisis response and consultancy services as a preferred partner for Fortune 500 corporations. With a uniquely integrated and scalable platform, Crisis24 has an unrivaled financial profile that enables greater investment in technology than industry peers.

Learn more at crisis24.com

EMAIL OR VISIT US AT:
INFO@CRISIS24.COM
CRISIS24.COM

Winding highway through the mountains at night.