Securitas

Risk Intelligence Center

Annual Intelligence Estimate

2026 Estimate

January 2026

intelligence@securitas.com

Contents

Introduction

Mike Evans

Director, Risk Intelligence Center

BRAVE NEW WORLD: WHERE THERE IS RISK, THERE IS OPPORTUNITY

Never before has there been a time and a place where both Security and Risk are required to go further, faster, and be better future-proofed, to safeguard organizations. Security is not a 'cost center,' it is a strategic enabler to 'do business,' and Risk is not a means of managing that 'cost,' it is a decision-making capability. Security and Risk, when driven as part of an Intelligence-led strategy, provides organizations with the advantage and confidence they need to manage risk and realize opportunities.

Events in the final days of 2025 — and the first of 2026 — set the tone for the Risk and Security landscape in the coming year:

- **Unlikely does not mean impossible:** (Re) viewing low-probability high-impact risks as a question of "when, not if?" and preparing for worst-case scenarios helps achieve the best possible outcomes.
- **Divergence is driving convergence:** The world is changing. Organizations are being directly (and indirectly) impacted by global and local events, physically and digitally, whether they realize it or not, and situational awareness and understanding is key to an effective response.
- **Security is a strategic enabler:** Where there is risk there is opportunity, and with new markets opening (and closing), changing consumer appetites and public sentiment, Security and Risk is essential to safeguarding organizations and enabling them to meet their objectives.

From a decision maker's perspective, the current climate is typically considered 'High Risk / High Reward'. However, another way to view this is 'Managed Risk / Maximum Reward' – a key theme for organizations in today's uncertain global risk landscape, and core to the Securitas Risk Intelligence Center (RIC) Annual Intelligence Estimate 2026.

WHAT IS THE SECURITAS RIC ANNUAL INTELLIGENCE ESTIMATE?

The Securitas Risk Intelligence Center's (RIC) Annual Intelligence Estimate provides actionable intelligence for corporate security and security risk professionals for the year ahead – and beyond.
The Annual Intelligence Estimate includes:

- **Strategic Security & Risk Driver Analysis** identifying key themes, trends, patterns, and emerging signals shaping the security and risk landscape in 2026.
- **Corporate Security Intelligence Assessments** applicable to organizations of every industry and location, including threat and protective intelligence analysis.
- **Global Risk Intelligence Assessments** covering global, regional and local intelligence concerns, including geopolitical threat and risk analysis.
- **Wildcard Scenario Analysis** exploring a selection of high-impact / low-probability scenarios with far-reaching implications for organizations.
- **Key dates in 2026** highlighting flashpoints of heightened threat and risk associated with scheduled events, including geopolitical, political, and social events.

The report is intended as an actionable alternative to other thematic assessments, with security decision makers in mind. The Annual Intelligence Estimate bridges the gap between strategic risk assessments intended for an executive audience, and tactical analysis meant for the frontline, to support those who are responsible for safeguarding their people, property, and whatever else matters most.

The Annual Intelligence Estimate provides situational awareness and understanding for organizations in all industries and sectors, and as such is produced as a digestible high-level brief for a general audience complete with practical considerations. The RIC also produces organization-specific, industry-relevant, and geographically-tailored assessments, which are available upon request.

If you have any questions about this report, or if you would like to discuss your specific intelligence requirements, please contact the RIC.

Our intelligence toolkit

Awareness

Regular scheduled & ad hoc reporting on the global security and threat landscape. Including Intelligence reports (INTREPs) and situation reports (SITREPs)

- Daily Global Intelligence Reports
- Weekly Global Intelligence Outlooks
- Monthly Threat Forecasts
- Monthly Intelligence Summaries (INTSUMs)
- Situation Reports (SITREPs) and Intelligence Reports (INTREPs) for significant developments

Alerting

Geo-targeted email-based alerts for security and threat events nearby. Fully customizable based on severity, proximity, and frequency with incident types:

- Criminality
- Civil unrest
- Terrorism
- Weather
- Travel and transportation

Advisory

An **all-in-one** Protective, Threat, and Risk Intelligence solution for your organization, operations, and brand. Includes:

- Monitoring for your specific requirements
- Daily Monitoring intelligence summaries
- Immediate briefs for warnings intelligence
- Threat, Protective & Risk Intelligence solution
- Access to the on-demand Ad hoc reporting service

Analyst

Dedicated intelligence resources complete with Securitas' Global Intelligence Community expertise.

Equipped with all the tools and training to support your intelligence requirements and protect your organization.

Ad Hoc Intelligence

Subject matter expertise and consultancy for any dynamic specific intelligence requirements
Common report types include but are not limited to:

- Travel & traveler security report: In-depth analysis of travel safety and security threats.
- Executive protection & Defensive Screening: information vulnerability assessment of a target Principal (i.e. an executive).
- Event Security Assessments & Screening: Due diligence & live monitoring.

Meet the team


ALEX JOHNSON


ALMA ABRAHAM


ANASTASIA JOBARD


BEN GIDDINGS


CIAN LYNCH


FREDDIE VENABLES


JOHN COUDRIET


JOSHUA MENDELSON


JUANITA JOHNSON


KIMBERLEY DEAN


LAURA STEVENS


LOUISE MARTIN


LUCY DICKENS


MATT PHILLIPS

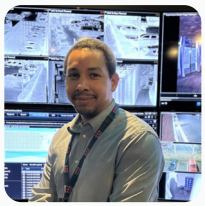

NATHAN SKEET


NICK FULLICK


OLIVER BACCHUS


SOPHIE CAIRNEY


CHARMIAN TAYLOR


PIERS REGISTER


ALEX BLITZ


JESS WILSON


JOE BECKFORD


OZICHI EGEONU


MIKE EVANS

Approach

The RIC employs an all-source intelligence strategy, utilizing all available and appropriate sources of intelligence based on the intelligence requirement(s).

This approach combines the expertise of our in-house analysts, the global network of the Securitas organization, third parties and partners, and cutting-edge technology for open-source intelligence (OSINT), to produce the highest quality finished intelligence. Inclusion in the Annual Intelligence Estimate is not a statement that any of these scenarios will occur, but that the potential exists for the threat to manifest and that the threat should be considered when performing security and safety reviews and risk assessments.

Threat levels

This report uses the RIC's threat level system to score threats on a 1-5 scale based on the assessed likelihood and severity, and / or intent and capability.

5 - EXTREME	Very high / extreme threat. Review and respond if required.
4 - HIGH	High / major threat. Consider taking appropriate action.
3 - MODERATE	Moderate threat. Maintain awareness, consider precautions.
2 - LOW	Low / limited threat. Be advised.
1 - VERY LOW	Very low / insignificant threat. For awareness.

Language of probability

This report uses the RIC's language of probability to provide an assessment of the likelihood of a threat manifesting, based on probability, using a percentage, fraction, or ratio as a baseline. This helps to provide context and clarity, and helps promote a standardized understanding of assessment and terms used.

Term	Probability
Remote	0-5%
Highly unlikely	10-20%
Unlikely	25-35%
Realistic possibility	40-50%
Likely/Probable	55-75%
Highly likely	80-90%
Almost certain	95-99%

Intelligence cut off date (ICOD)	**0000hrs UTC 05 January 2026**

Trends, patterns, & influencing factors

The RIC's Annual Intelligence Estimates from 2023, 2024, and 2025 highlighted a variety of trends and patterns within the global security threat landscape, all of which have had and continue to have direct impacts on organizations, including their security, operations, and brand and reputation. Some of these threats have overlapped in recent years, advancing and evolving to encompass new threat actors, tactics, and targets, with entirely new threat vectors and Strategic Drivers also being brought to the forefront. Organizations have increasingly faced heightened threats and enhanced risks as a result of the evolving global security threat landscape, further promoting the necessity of proactive intelligence to inform organizations of the most pressing threats.

The Corporate Security threat / risk scenarios included in the RIC's Annual Intelligence Estimates from 2023, 2024, 2025, and 2026 aim to provide organizations with a proactive decision-making advantage to limit potential impacts of the global security threat landscape, with the main themes outlined below:

2023

- ESG initiatives incite backlash and security threats
- Chronic stresses of climate change and the acute shocks of natural disasters
- Balancing health security versus hypersensitivity
- The ever-evolving cyber threat landscape
- Information disorder and the increasing real-world threat of 'fake news'
- The expanding activist landscape
- (R)evolution in terrorism and extremism
- Espionage targeting organizations and their assets
- Energy resilience and security
- Threats to global supply chain resilience and security

2024

- Converge of geopolitical and sociopolitical threat actor motivations
- Chokepoints and great power competition disrupt supply chains
- 2024 super election cycle
- Artificial intelligence arms race
- Climate and environmental risks reach new limits
- Supercharged cybercrime
- Global impacts of China's economic downturn
- ESG backlash turns from bark to bite
- Critical infrastructure to remain a critical vulnerability
- Increasing corporate espionage shifts focus to counter-intelligence

2025

- Changing 'rules-based order' heightens concerns over possible collapse
- Heightened gray zone warfare and sabotage threaten organizations' security
- Organizations increase preparations for 'wartime scenarios'
- Executives and politicians in the crosshairs of threat actors
- AI faces its watershed moment
- Ideological insiders increasingly threaten organization security
- The growing overlap in threat actor motivations
- Exploitation of drones for hostile purposes
- Social media exploitation fuels information disorder
- Impacts of health security events ripple across supply chains

2026

- Threat actors target CNI to maximize impact
- Backsliding corporate progress on ESG challenges drives activism
- Mass layoffs linked to AI heighten anti-corporate sentiment and insider risks
- Rise in protectionist policies to safeguard sovereign resilience
- Threat actors exploit vulnerable public and private events
- Sustainability concerns disrupt resource-intensive infrastructure projects
- Authorities' response to drone threat encourages further exploitation
- Risks to organizations from increased dependency on cloud environments
- Information landscape threatened by emerging GenAI
- Social media increasingly weaponized to facilitate mass doxxing campaigns

Strategic risk drivers

P Political

STRATEGIC DRIVERS IDENTIFIED IN 2025

- US presidential transition drove a shift toward 'geopolitical transactionalism,' straining traditional alliances.
- Country / regional instability (largely fueled by conflict) continued to involve international powers and influence domestic politics and security in 'unaffected' nations.
- Intensifying great-power competition, particularly China-US and Russia-West, drove foreign policy recalibration across regions and increased gray-zone warfare (GZW) activities.

EXPECTED STRATEGIC DRIVERS IN 2026

- Democratic backsliding and governance challenges (including corruption, erosion of the rule of law) are likely to increase the probability of unrest.
- Radical politics becomes increasingly mainstream in the West, driving swift regulatory changes, unrest, and polarized discourse, leading to the targeting of organizations and high-profile individuals.
- Rise of the 'strongman' leadership style, prioritising unilateral action, continues to reinforce 'might-is-right' dynamics, increasing risk of escalatory behavior, miscalculation, and conflict.

E Economic

STRATEGIC DRIVERS IDENTIFIED IN 2025

- Protectionist trade measures caused significant supply chain disruptions, increased costs, and reduced investor confidence.
- Inflation eased in many regions, but high living costs and wage stagnation fueled labor unrest and strikes globally.
- Fluctuating energy markets, driven by conflict, production cuts, and sanctions, resulted in unpredictable operating costs for energy-intensive industries.

EXPECTED STRATEGIC DRIVERS IN 2026

- Continued fragmentation of global trade, driven by protectionism and political uncertainty, is likely to raise operational costs and complicate market access.
- Competition for critical minerals and technology manufacturing capacity will intensify, influencing economic alliances
- Fiscal constraints due to high public debt have a realistic possibility of forcing austerity measures, increasing the risk of unrest.

S Social

STRATEGIC DRIVERS IDENTIFIED IN 2025

- Gen Z-led digital mobilization drove decentralized protests across the Global South, focused on distinct and overlapping grievances, including corruption and high youth unemployment.
- AI-driven job displacement became a high-profile public concern, as corporate layoffs were explicitly linked to the implementation of autonomous systems and AI agents.
- Migration and border control remained an acute security priority, with large-scale displacement from ongoing conflicts and climate-change-driven natural disasters.

EXPECTED STRATEGIC DRIVERS IN 2026

- A global generational divide will deepen, with younger populations demanding more social equity, leading to increased physical and digital activism across the Global South.
- Social cohesion is likely to deteriorate further as online information disorder, economic pressures, and political distrust fuel polarization and extremist narratives.
- Reduction in global aid budgets is likely to strain humanitarian efforts, increasing health and displacement risks.

This Political, Economic, Social, Technological, Legal, and Environmental (PESTLE) analysis outlines the key external factors that have been identified as shaping the business operating environment in 2025, and those that are expected to be observed in 2026. It highlights the drivers influencing organizational strategy, risk exposure, and decision-making for businesses across the globe in all sectors.

The analysis highlights how geopolitical instability, economic volatility, societal change, technological dependence, regulatory complexity, and environmental stressors interact to create risks and opportunities for organizations.

By identifying current strategic drivers and their expected impacts, this analysis provides a structured overview of macro-level trends that organizations must monitor, adapt to, and incorporate into long-term planning and resilience strategies.

T Technological

STRATEGIC DRIVERS IDENTIFIED IN 2025

- The interconnected information technology infrastructure vulnerability was exposed by multiple widespread internet outages, for example, Cloudflare and major data center failures.
- Surge in high-profile cyber attacks, with ransomware and supply chain intrusions, caused major operational outages across sectors.
- Competition over critical minerals key for advanced technologies and semiconductors persisted, shaping national security policy.

EXPECTED STRATEGIC DRIVERS IN 2026

- As nations increasingly assert sovereignty over AI systems, organizations will face an increasingly multipolar digital order, including divergent security requirements, regulations, and compliance across different regions.
- Accelerating development of quantum technologies intensifies geopolitical competition, prompting increased export controls while raising long-term security risks for organizations.
- Manufacturing reshoring increases corporate operating costs but strengthens supply chain security.

L Legal

STRATEGIC DRIVERS IDENTIFIED IN 2025

- Global governance structures faced increased push-back and non-compliance, influencing breakdowns and violations of international laws.
- Expansion of international sanctions regimes against strategic industries and nation-states continued to escalate, creating operational and travel risks for businesses.
- Regulatory lag of high-risk technologies, including AI, enabled exploitation by malicious actors and created compliance uncertainty.

EXPECTED STRATEGIC DRIVERS IN 2026

- Legal accountability for cyber negligence, data breaches, and environmental harms will continue expanding, increasing financial and reputational risks for organizations.
- Legal disputes over territorial claims, maritime rights, and resource access are likely to increase, affecting maritime routes and multinational risk exposure.
- Expanding state use of emergency powers, often introduced during periods of unrest, is likely to complicate business operations and erode civil liberties.

E Environmental

STRATEGIC DRIVERS IDENTIFIED IN 2025

- Pressure on water resources reached severe levels in several key economic zones (e.g. Southern Europe, South Asia) triggering localized agricultural and industrial shutdowns.
- High-profile legal cases scrutinizing organizations alleged greenwashing claims set a precedent, creating brand reputational risks.
- A continuation of extremely high global temperatures, heatwaves and extreme weather events caused severe infrastructure damage and supply chain issues.

EXPECTED STRATEGIC DRIVERS IN 2026

- Organizations perceived to be complicit in causing climate degradation will face heightened threats of legal action and protests.
- Extreme weather events and natural disasters increase in frequency / intensity, disrupting global logistics networks, damaging energy infrastructure, and threatening workforce safety.
- Climate-driven resource scarcity will exacerbate cross-border tensions and increase risks of conflict.

Corporate security

1

Threat actors target CNI to maximize impact

Attacks targeting Critical National Infrastructure (CNI) have steadily increased throughout 2025, with hostile threat actors exploiting both kinetic and non-kinetic tactics, techniques, and procedures (TTPs). As global tensions over multiple flashpoints have escalated, state-sponsored / gray zone warfare (GZW) threat actors, activist groups, extremist organizations, and lone actors have continued to target traditional CNI, such as energy, water, and communications, as well as non-traditional targets, such as data centers and airports. Ease of access to cyber threat tooling, as well as the prevalence of commercially-available unmanned aerial systems (UAS), have allowed threat actors to maximize impact on CNI with minimal outlay.

- Hostile threat actors are almost certain to continue targeting CNI, both using traditional TTPs such as physical sabotage and via non-kinetic TTPs such as malware and cyber attacks.
- Nation-states are likely to increase the usage of proxy threat actors such as organized crime groups (OCGS) to conduct sabotage and disruptive attacks targeting CNI to maximize political pressure, destabilize enemy nations, and spread uncertainty, while enhancing deniability.
- Radical activist organizations are likely to increase physical sabotage and cyber attack campaigns targeting CNI operated or supported by organizations deemed as acting against group goals, with the intent to cause widespread disruption.

Scenario	Scenario condition	Assessed likelihood
An improving geopolitical and socio-political outlook drives a decrease in CNI targeting, chiefly due to reduced activist desire and intent. Nations reduce the use of proxy actors to conduct GZW actions as tensions ease.	Improves	Highly unlikely (10%)
Global tensions continue to rise, centered around ongoing conflicts and flashpoints, including environmental, social, and economic (ESG) issues; activists increasingly target CNI to increase exposure for their causes.	Baseline	Likely / Probable (55%)
Geopolitical tensions escalate further, driving more nation-states to engage in increasingly direct targeting of CNI, including deployment of proxy assets as part of wider attack methodologies.	Worsens	Unlikely (35%)

Advisory

- Assess the organization's exposure (both direct and indirect, such as through supply chain partners) - to operational impacts resulting from disruption to CNI.
- Ensure failsafes and mitigations related to key supply streams (such as energy, water, telecoms etc) are in place, allowing for resilient operational processes and capabilities should CNI availability be impacted.
- Monitor and maintain awareness of regions prone to geopolitical upheaval or disruption, particularly where those regions are linked to operational stability. Monitor government advisory notices within those areas.

Indicators	Implications
— Increased rhetoric surrounding global trade, specifically related to tariffs, sanctions, and access to rare minerals. — Increased tensions across state borders around politically volatile regions. — More frequent and widespread use of UAS by threat actors over restricted airspace. — Increased social media reporting highlighting successful CNI attacks by activist groups. — Increased digital communication by activist groups advising on attack methodologies targeting CNI or promoting sites.	— Organizations responsible for or with links to CNI face a greater risk of being targeted by threat actors. — Reduced access to critical materials over increasing isolation stemming from deniable GZW hostile activity targeting CNI. — Disruption to daily operational capabilities from impacts to communication CNI — Increased expense requirement and legal responsibility related to managing and operating CNI facility contracts. — Loss of critical data and information, and increased dependence on external factors to maintain data integrity related to data center CNI.

Backsliding corporate progress on ESG challenges drives activism

Activist groups continue their persistent targeting of companies perceived to be violating environmental, social, and governance (ESG) commitments through protracted boycotts, demonstrations, and online criticism. Organizations have been accused of delaying net-zero targets or amending diversity, equity, and inclusion (DEI) policies in response to political and economic pressures throughout 2025, and these accusations will almost certainly persist – and likely increase – throughout 2026. Activist groups will continue targeting firms with increasingly innovative and disruptive measures to achieve their goals, in particular focusing on organizations – and individuals – who are perceived to be walking back prior ESG commitments.

- Environmental / anti-war / social justice groups will likely launch and / or bolster boycott, divestment, and sanctions (BDS) campaigns targeting organizations perceived to be taking lower-visibility stances on ESG.
- Organizations targeted by these actions face the risk of operating in a polarized working environment, creating conditions with the potential to motivate internal threat actors to organize campaigns, leak internal communications, and engage in whistleblowing activities.
- Organizations are unlikely to be able to quietly scale back on ESG commitments without generating increased scrutiny from activist groups. External pressures from shareholders, policymakers and investors will likely push organizations to de-prioritize or abandon prior ESG initiatives, risking further targeting.

Scenario	Scenario condition	Assessed likelihood
Reduction in activist targeting of companies delaying or scaling back ESG commitments as activist groups prioritize other causes.	Improves	Highly unlikely (10%)
Organizations scaling back ESG priorities continue to be targeted as activists use open source data to investigate companies, using social media to organize BDS campaigns and protests.	Baseline	Likely / Probable (60%)
Activist groups do not see sufficient progress with existing approaches, and escalate to more disruptive tactics, such as vandalism, building occupation, or threatening the physical security of company executives in order to apply pressure.	Worsens	Unlikely (30%)

Advisory

- Consider the risks of making public or official statements regarding divisive or controversial subjects. These may draw attention from more committed threat actors, who may be more likely to engage in hostile or disruptive actions.
- Monitor and assess workforce sentiment following announcements and communications around ESG or similarly emotive or divisive topics to identify early indications of dissatisfaction and / or potential insider threat vectors.
- Identify and monitor threat actors who may be incited / influenced / inspired to engage in hostile targeting (directly or indirectly) based on planned organizational policies and initiatives.

Indicators	Implications
— National-level policymakers applying further pressure on organizations to walk back or abandon ESG initiatives. — Activist movements expanding targeting to include secondary / tertiary entities associated with organizations accused of de-prioritizing ESG initiatives (such as supply chain partners, insurers etc). — Increased activist focus on individuals (CEOs, Exec suite) as opposed to just 'whole organization' targeting. — Established activist groups announcing new campaigns (or expansions to existing campaigns) focused on ESG 'walkbacks'.	— Organizations will need to balance external pressures from stakeholders and policymakers against external (and internal) pressures from activist groups when communicating policy changes. — Increased physical security costs for executives and at site locations (including events such as AGMs) during periods of significant criticism. — Organizational partners (such as charities / non-profits etc) may perceive ESG 'walkbacks' negatively, leading to public criticism or termination of partnerships. — Persistent activist targeting and / or negative discourse around organizations can impact consumer / market confidence, reducing business revenues.

Mass layoffs linked to AI heighten anti-corporate sentiment & insider risks

AI-driven restructuring and mass layoffs are expected to continue throughout 2026 as organizations deepen their transition toward automation, generative AI deployment, and data-center expansion, while correcting for pandemic-era overhiring. These reductions are likely to intensify anti-corporate sentiment, elevate insider risks, and drive agitation among anti-AI activist groups and labor-rights networks. These conditions create heightened vulnerability during periods of workforce disruption, while activist networks increasingly organize opposition to rapid AI adoption.

- AI-driven workforce reductions, mainly in tech, manufacturing, customer service, and logistics, are heightening insider risks such as data theft, sabotage, and misuse of AI tools. The growing sophistication of these tactics poses an escalating threat to financial, legal, and reputational stability, while anti-AI and labor-rights groups are likely to intensify pressure through online campaigns and strikes.
- Localized insider incidents are a realistic possibility, while large-scale unrest remains unlikely; however, non-trivial operational impacts to data centers, digital services, and automated production environments from broader actions relating to anti-AI sentiment (including non-insider actions) are possible.
- Insider sabotage within AI-enabled environments has the potential to trigger organization and sector-wide disruptions, while the growing complexity of activist strategies and tactics and rising insider-risk factors present an escalating threat to operational stability in industries undergoing rapid AI-driven transformation.

Scenario	Scenario condition	Assessed likelihood
AI-driven layoffs ease as workforce planning stabilizes, reducing insider-risk exposure and lowering anti-corporate sentiment.	Improves	Highly unlikely (10%)
AI-related restructuring continues at a steady-moderate pace, maintaining moderate insider risk, ongoing online criticism, and periodic activist pressure.	Baseline	Realistic possibility (50%)
Visible or repeated layoffs escalate anti-corporate sentiment, driving increased insider incidents and more coordinated activist campaigns targeting corporate assets and reputation.	Worsens	Realistic possibility (40%)

Advisory

- Maintain an enhanced security posture by strengthening insider-threat monitoring, tightening access controls, and increasing visibility over AI-enabled systems to reduce opportunities for misuse or sabotage during workforce disruptions.
- Engage regularly with authorities and regulators to receive updated guidance and coordinate on preventative measures, ensuring facilities, data centers, and automated environments are protected against emerging threats.
- Reinforce operational and supply-chain resilience by identifying critical dependencies, reviewing contingency plans, and preparing alternatives to mitigate disruptions from insider actions or activist interference.

Indicators	Implications
— Increasing AI-linked workforce reductions across tech, manufacturing, and service sectors in regions with advanced automation. — More organizations publicly championing and promoting their use of AI tooling in roles previously carried out by human employees. — Growing public, political, and activist commentary criticizing rapid AI adoption, with organized labor groups coordinating campaigns against corporate automation strategies. — Rising insider-risk incidents, including data theft, misuse of access, or sabotage linked to displaced or dissatisfied employees.	— Increased security requirements and budgets, particularly for insider-threat monitoring, access controls, and protection of AI-enabled infrastructure. — Greater likelihood of operational disruptions, including data-center outages, supply-chain breakdowns due to insider sabotage or external activist actions, or interference with automated production environments. — Elevated regulatory and reputational risks, prompting companies to strengthen employee-impact planning and public communication around AI adoption.

Rise in protectionist policies to safeguard sovereign resilience

The rise in protectionist policies, driven by escalating geopolitical tensions, national security considerations, and sovereignty objectives, has heightened market volatility and introduced greater economic uncertainty for organizations through 2025. This trend is expected to continue through 2026, reflecting governments' increasing use of trade as a tool for political leverage and the domestication of manufacturing / services to strengthen national security and sovereign resilience.

— Global leaders will likely continue implementing protectionist policies as geopolitical and socio-political tensions continue. This approach will likely continue to exacerbate existing issues, such as supply chain vulnerabilities, trade agreements being used as a negotiating tactic, and embargoes / tariffs on key resources.

— The long-term impacts of widespread protectionist policies has the potential to drive shifts in corporate strategy as cross-border trade becomes more challenging and / or costly. This can lead to organizations exploring 'in-country' solutions, further degrading global trade relations and exposing adapting supply chains to threat actors.

— The reshoring of industries essential to the preservation of defence capabilities and the maintenance of critical national infrastructure (CNI) will likely remain a focal point of future protectionist policies. However, this may in turn drive up costs and expose organizations to complications arising from rapid shifts in supply and demand.

Scenario	Scenario condition	Assessed likelihood
Geopolitical and socio-political tensions ease, reducing market volatility. Cross-border trade stabilizes, with a downward trend in the use of tariffs and embargoes.	Improves	Highly unlikely (15%)
Political leaders continue to impose sporadic protectionist policies, forcing organizations to continuously adapt operations and reassess commercial relations, causing uncertainty.	Baseline	Likely / Probable (55%)
Trade is increasingly used as political leverage, creating unmanageable uncertainty in global markets. Supply chains are significantly disrupted due to rapidly changing trade conditions.	Worsens	Unlikely (30%)

Advisory

— Ensure all operations are receptive and adaptable to regulatory changes and establish realistic contingency plans should protectionist policies impact operational capability or capacity.

— Implement robust security procedures surrounding supply chains and stockpiles to prevent threat actors from exploiting vulnerabilities during transitional periods following the announcement of such policies.

— Liaise with international partners to establish incident response plans (IRPs) that allows operational continuity despite uncertainty.

Indicators	Implications
— A regional increase in nationalist populism advocating for the anti-globalization of industries. — More frequent cancellation of contracts citing security concerns. — Controversial behavior by areas / organizations that other countries do not want to be deemed complicit in. — Global flashpoints necessitating political negotiations. — Increasing protectionist policies by economic allies inspiring retaliatory policies. — Increasing concerns around data access and espionage from imported goods.	— Degradation of cross-border cooperation, stunting innovation and development within targeted industries. — An increasing value of imports / exports exploited by threat actors converging both cyber and physical aspects to remain undetected. — Sustained uncertainty regarding profits, supply-demand, and regulatory standards. — Significant decline in foreign direct investment (FDI). — Broader financial and operational consequences for affiliates, investors, and third-party vendors as expectations are balanced with policy.

Threat actors exploit vulnerable public and private events

Threat actors have increasingly targeted large-scale events in recent years due to their accessibility, the prospect of high-value targets (HVTs) in attendance, and the opportunity to publicize their actions to gain traction on social media. Ongoing geopolitical tensions and divisive sociopolitical issues, such as environmental protection and the development of artificial intelligence (AI), will remain key drivers for activism and insider threats through 2026. In addition to existing tactics, techniques and procedures (TTPs), threat actors will almost certainly continue to evolve their approach through innovative methods, such as exploiting elevated concerns as an opportunity to issue hoax threats and cause disruption.

- Whilst targeting of events based on corporate attendance has been utilized by activist groups for many years, other threat actor profiles are increasingly likely to adopt the tactic as a method of gaining access to key individuals or assets in a less controlled environment.
- The attendance of large organizations during events raises the prospect of corporate espionage of sensitive information, potentially later utilized to inflict reputational damage, blackmail or sell to competing companies.
- Increasingly resourceful threat actors are likely to utilize multiple data sources to gather information on their target, such as identifying hotels close to an event where a target may likely be staying, or likely transport routes to and from the event. This can then be used to carry out actions linked to, but away from the event itself.

Scenario	Scenario condition	Assessed likelihood
Improved security posture for events and associated HVTs drives threat actors into pursuing other avenues of attack due to lower perceived success rates. Reduced disruption to events from threat actor targeting.	Improves	Highly unlikely (10%)
Threat actors continue to target and disrupt events, employing new and existing TTPs. Events continue to face disruption both from threat actor intervention and from heightened security protocols.	Baseline	Likely / Probable (60%)
Threat actors achieve repeat success from targeting events. Perception of greater success drives further attempts, heightening disruption. Significant impacts to even non-target events due to increased security measures responding to the elevated threat.	Worsens	Unlikely (30%)

Advisory

- Enhance operational security (OPSEC) around attendance at external events, reducing the publicization of specific event details (such as attendees). Avoid publicly sharing details such as event passes / accreditations on social media.
- Consider appropriate background checks on attendees to reduce the possibility of threat actors gaining legitimate access to an event.
- Ensure that security arrangements for HVTs do not begin and end ‘at the door’, considering the potential for threat actors to engage in targeting outside, near, or on the way to and from the event.

Indicators	Implications
— Increased targeting of accounts linked to events on social media based on individuals or organizations attending the event. — Increasing reports of events being attended / targeted by non-activist threat actors, such as disgruntled customers, criminal elements and fixated individuals. — Escalation in the TTPs used by threat actors seeking to disrupt events. — Flashpoints in driving factors (such as geopolitical conflicts) in the runup to or during events. — Boycott movements targeting secondary / tertiary organizations, as well as event holders and hotels hosting attendees.	— Enhanced security requirements for those hosting or attending events resulting in increased security budgets. — Stricter application and vetting processes for attendees impacting accessibility to the public and external organizations, potentially driving criticism. — Organizations increasingly consider switching events to online platforms to minimize the possibility of disruption. — Organizations become reluctant to send high-profile executives to public events due to security concerns.

Sustainability concerns disrupt resource-intensive infrastructure projects

The demand for resource-intensive infrastructure projects such as data centers, renewable energy generators, and semiconductor plants will increase throughout 2026, with governments subsidizing projects for strategic and economic reasons, and organizations continuing to transition to AI-driven services and operations. These projects demand substantial resources, including energy, water, land, and critical minerals, increasing sustainability concerns from regulators, political leaders, and socio- and economic- actors including environmental activists and the workforce.

- This growth is driven by the AI / digital 'arms race' at the strategic geopolitical level, and at the market-level with organizations driving their AI and digital strategies for competitiveness – increasing demand for data centers and semiconductors – as well as ongoing transitions to clean energy technologies such as electric vehicles and renewable power generation, which require critical minerals.
- The resource intensity of these infrastructure projects has triggered protests, sabotage, lawsuits, and investigations by activists, regulators, and governments due to their impact on water supply, energy resources, land availability, and waste. Additionally, they are high value targets (HVTs) for nation-state actors and espionage and sabotage tactics, which though not motivated by sustainability concerns, highlights the sector criticality.
- Continued expansion of these projects in 2026 will lead leading to growing pressure on developers and governments to implement more stringent environmental restrictions, risking delays to digital / AI transition plans, and tighten approval processes for future projects, despite perceived backsliding on ESG commitments globally.

Scenario	Scenario condition	Assessed likelihood
Technological breakthroughs or global demand changes lead to a reduction in resource-intensive infrastructure projects, reducing sustainability concerns.	Improves	Highly unlikely (10%)
Global infrastructure demands continue at the current rate, leading to further expansion of construction projects, increasing scrutiny in both political and public discourse.	Baseline	Likely / Probable (65%)
Demand growth accelerates significantly, leading to increased strain on resources, prompting business disruptions, polarized political rhetoric, and heightened activism.	Worsens	Unlikely (25%)

Advisory

- Assess exposure to resource-intensive infrastructure, particularly within regions subject to heightened controversy surrounding resource strain and environmental harm.
- Maintain awareness of online sentiment regarding infrastructure projects, increasing local-level engagement to address concerns over sustainability, including transparent communication over resource requirements, project timelines, and economic benefits.
- Monitor potential changes to regulations around resource-use and environmental impacts to mitigate operational impacts to project timelines and supply chain disruptions.

Indicators	Implications
— Increased construction of new data centers, semiconductor-reliant products, and renewable energy projects. — Heightened scrutiny of water shortages, grid-capacity constraints, or land-use disputes around project sites, including in the news and on social media. — Increased protest activity, including local-level campaigns and lawsuits targeting projects and involved companies. — Increase in local jurisdiction moratoriums or blocking planned infrastructure projects due to local opposition. — Increasing conspiracy theory narratives surrounding associated infrastructure and technologies.	— Sustained scrutiny leads to policy changes and more stringent sustainability requirements. — Higher project costs and delays to infrastructure projects as regulations tighten and zoning approval processes become lengthier. — Companies reliant on this infrastructure face supply bottlenecks and unstable suppliers. — Increase in the frequency, scale, and intensity of activism against developers, exacerbating delays. — Increased threat of extremist acts including sabotage and destructive acts.

Authorities' response to drone threat encourages further exploitation

Continued hesitancy by Western authorities to confront threats posed by drones to transport nodes, military sites, and other pieces of critical national infrastructure (CNI), alongside technological advancements in unmanned aerial systems (UAS) will continue to provide threat actors (including activists, terrorists, and state-sponsored individuals) with opportunities to engage in disruptive actions throughout 2026. Increases in unauthorized drone activity over sensitive sites in recent years have raised concerns over the wider impacts on affected entities, contributing to increased uncertainty amid criticism of authorities' capacity to address perceived hybrid threats.

- The commercial availability and advancements in UAS capability will drive further evolution of tactics, techniques, and procedures (TTPs) in drone deployment, with threat actors, including criminal organizations, utilizing locally launched, expendable hardware to target residential, recreational, commercial, and industrial sites.
- Highly motivated individuals will continue to display their capacity to use UAS as an alternative form of protest, exploiting anxiety to maximize publicity and raise awareness, as well as to record assets, evidence claims, and lend credibility to critical narratives.
- The impact of operational disruptions due to suspicious drone sightings around CNI and transport nodes will likely continue to be exploited and weaponized by hostile state actors seeking to engage in hybrid or gray zone (GZW) warfare.

Scenario	Scenario condition	Assessed likelihood
Widespread deployment of specialist counter-drone equipment, as well as provisions ensuring affected parties have the authority / capacity to intercept drones safely. Authorities implement clear rules of engagement for suspicious UAS activity.	Improves	Highly unlikely (10%)
Adversaries continue to exploit hesitancy, testing drone detection / response capabilities, and commitments to collective defense agreements, shaping thresholds for engagement.	Baseline	Highly likely (80%)
Escalation caused by a drone collision (accidental or deliberate). Failure to implement effective deterrents leads to increased impacts to CNI and transport hubs from UAS and 'jamming' systems leads to more widespread deployment by hostile actors.	Worsens	Highly unlikely (10%)

Advisory

- Conduct review of aerial reconnaissance vulnerabilities, ensuring procedures for airspace incursions above sites are implemented, and confidential assets are hidden from view.
- Maintain familiarity with regulations governing airspace restrictions above property, ensuring staff are trained and equipped for dealing with situations relating to UAS deployments (including cases such as 'security auditors').
- Maintain awareness of online footage disclosing site perimeters / on-site security measures that is likely to inform offensive activity, further reconnaissance, and or protests / direct action.

Indicators	Implications
— Increased use of drones for hostile reconnaissance to inform actions targeting sites. — Increased availability and access to UAS technology, particularly units which could be perceived as cheaper or ‘disposable’. — Heightened awareness and continued escalation contribute to increased reports of suspicious drone activity attributed to hostile state actors, increasing appetite for UAS detection systems. — Continued contestation of provisions for military authorities to address drone threats, particularly around sensitive sites adjacent to civilian populations in urban areas	— Continued risk of airspace closures as a result of suspicious drone activity, with non-malicious actors inadvertently causing disruption amid heightened anxiety. — Growing scrutiny on commercial drone detection systems, particularly technology developed by companies based in states perceived to be hostile by Western governments. — Heightened appetite for anti-drone investment to protect critical offshore assets / transit lanes. — Online exposure of in-place security measures potentially being exploited by other threat actors.

Risks to organizations from increased dependency on cloud environments

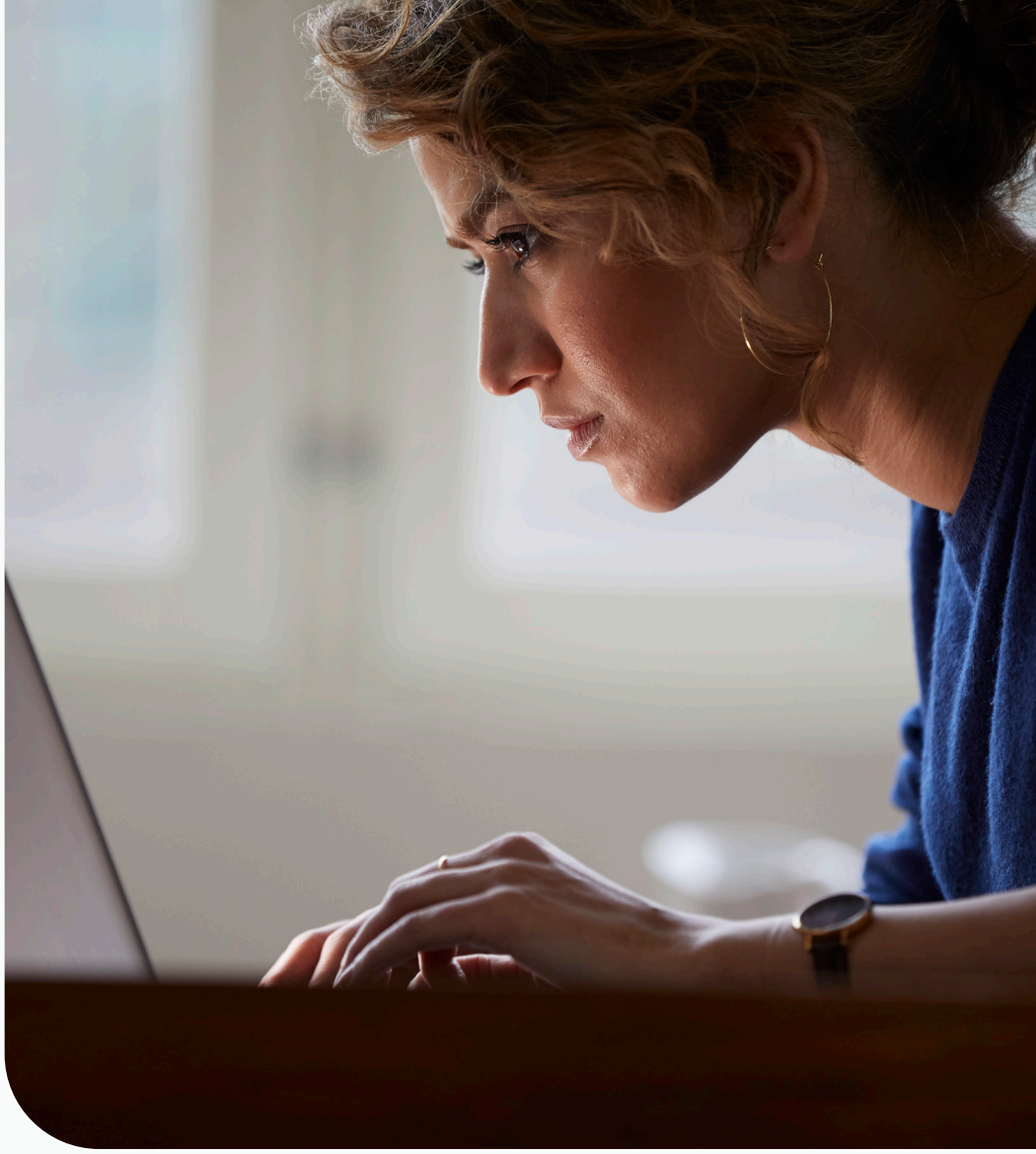
Cyber threats for businesses will increase as more companies migrate their operations to cloud-based Software as a Service (SaaS) models, increasing exposure to threats associated with cloud services, such as outages, breaches and misconfigurations. Digital infrastructure is monopolized by major cloud providers, such as Amazon Web Services (AWS) / Microsoft Azure / Google, but companies often use multiple platforms, increasing their exposure to digital risks, especially as businesses consolidate hybrid working and Artificial Intelligence (AI) into their operations.

- Generative AI will increase the threat of credential theft and phishing as it makes these tactics more accessible and effective with automation, reducing the technical threshold for attacks to be viable.
- Cloud-based digital infrastructure is conducive to these types of attacks as criminals can exploit human error by operating quickly, making detection and prevention challenging, and leaving large amounts of sensitive, unencrypted data vulnerable.
- The rapid migration by companies to multiple SaaS providers will continue to create considerable blind spots around Identity and Access management (IAM) privileges, increasing cyber and insider threats.
- Cloud outages will continue to occur sporadically, severely disrupting company operations and increasing the likelihood of attacks seeking to exploit these outages.

Scenario	Scenario condition	Assessed likelihood
Organizations recognize the growing threat and invest sufficiently in cloud security, reducing the threat of data breaches. Suppliers improve security and technical failsafes to mitigate and avoid incidents.	Improves	Highly unlikely (15%)
Companies continue migration to SaaS cloud-based providers, increasing the global impact of security incidents and outages, creating ever more significant data breaches and cyber threats.	Baseline	Likely / Probable (70%)
Issues with cloud providers become more frequent, including large-scale data loss. Companies are forced to decouple their operations from cloud-based systems.	Worsens	Highly unlikely (15%)

Advisory

- Ensure all personnel, as well as third parties / vendors, are informed and up to date on data protection and cyber security processes and practices, such as password strength and identifying and verifying requests for credentials.
- Train employees in detecting AI-driven impersonation tactics, such as deepfake calls, phishing / vishing attempts.
- Invest in modern, automated cloud security tools, such as Cloud Security Posture Management (CSPM) and Multi-Factor Authentication (MFA).
- Ensure contingency plans and operational failsafes are in place to minimalize disruption during cloud outages.



Indicators	Implications
— Organizations accelerate the move towards multiple SaaS cloud systems. — Cloud outages and breaches occur with increasing frequency, resulting in multi-sector disruption and facilitating further opportunistic attacks. — Increasing desire by authorities and governments to legislate toward more robust security and technical measures to ensure continuity of provision and protection of data within cloud services, including significant legal and financial repercussions for failures. — A major attack, outage or breach results in industry uncertainty around over-migration toward cloud services.	— Cloud outages cause major disruption to business operations across multiple sectors, including government and critical national infrastructure. — Businesses face persistent threats from breaches and subsequent data leaks, potentially exposing them to significant legal costs, reputational damage, and likely loss of business. — Organizations face financial and reputational risks from failures to adhere to regulatory requirements such as data protection laws. — Businesses have to realign their security spending to mitigate the increased cyber threat and associated consequences

Information landscape threatened by emerging GenAI

Artificial Intelligence (AI) capabilities are advancing faster than society's ability to distinguish authentic content from fabrications. This technological acceleration is likely to collide with a sustained decrease in institutional trust, creating conditions where corporations face tangible and disruptive threats from reputation attacks, market manipulation, and operational disruption. The information landscape will continue to fracture, as traditional media sees a deterioration in credibility whilst the growing mainstream influence of unvetted alternative sources persists and likely increases further.

— Trust in – and engagement with - legacy media institutions has reached historic lows. This vacuum is increasingly being filled by influencers, civilian journalists operating without editorial oversight, and alternative media, with many commanding audiences larger than major newspapers and prioritizing engagement over verification.

— State and non-state actors possess sophisticated generative AI capabilities and have demonstrated intent to manipulate information environments. Alternative media ecosystems on platforms like Telegram, X, and emerging decentralized networks will likely serve as primary distribution channels.

— Voice cloning, face-swapping, and text generation tools allow any motivated actor to create convincing synthetic content of executives, officials, or public figures within hours. Corporations in 2026 and beyond will likely face regular synthetic media attacks, including those intended to disrupt operations or extract sensitive information.

Scenario	Scenario condition	Assessed likelihood
Detection technology keeps up with AI capabilities, limiting synthetic content's impact, and platform policies create effective barriers, as the public develops verification habits through media literacy.	Improves	Highly unlikely (20%)
Synthetic media attacks rise significantly but remain manageable, as detection struggles to match generation quality, yet offers some protection. However, high-profile corporate incidents continue to cause disruptions.	Baseline	Realistic possibility (40%)
Synthetic content overwhelms detection and verification systems, public trust erodes further. Attacks on organizations facilitated by generated content increase in both frequency and effectiveness.	Worsens	Realistic possibility (40%)

Advisory

— Implement multi-layered authentication for executive communications, including verified channels that stakeholders know to check during crises. Establish code word systems for sensitive communications that cannot be replicated in deepfakes.

— Develop tools for monitoring social and alternative media platforms for brand and executive mentions and identify processes for identifying / reporting / removing generated content.

— Limit executive exposure in uncontrolled settings likely to provide high-quality source material for deepfakes. Review public appearances and speaking engagements for recording controls.

Indicators	Implications
— Increasing prevalence and access to tools for generative media creation. — Alternative media creators' audiences surpass traditional news outlets, and platform algorithms prioritize content from civilian journalists and influencers over legacy media. — Corporate crises increasingly originate from alternative sources rather than traditional reporting. Verification standards decline, and synthetic media circulates widely before being debunked — Threat actor groups increasingly utilize GenAI capabilities to spread information disorder, enable hostile action and attack corporate reputations.	— Employee trust and morale suffer as synthetic content targets internal communications. Disaffected personnel amplify or even generate synthetic media to attack their own organization. — Insider threats increase as employees cannot verify leadership communications. — Conspiracy theories and deepfakes undermine public and economic trust. — Synthetic media campaigns target supply chain partners with false claims about quality, safety, or business practices. B2B relationships suffer if authentication of partner communications becomes unreliable.

Social media increasingly weaponized to facilitate mass doxxing campaigns

The use of social media to facilitate mis / dis / malinformation campaigns has increased significantly in 2025 as the speed and scale at which narratives can be created, amplified, and weaponized has been enabled by improvements in generative AI technology. This rapid amplification can also drive targeted doxxing, as false or inflammatory content is used to justify exposing an individual's personally identifiable information (PII) on social media and mobilize harassment.

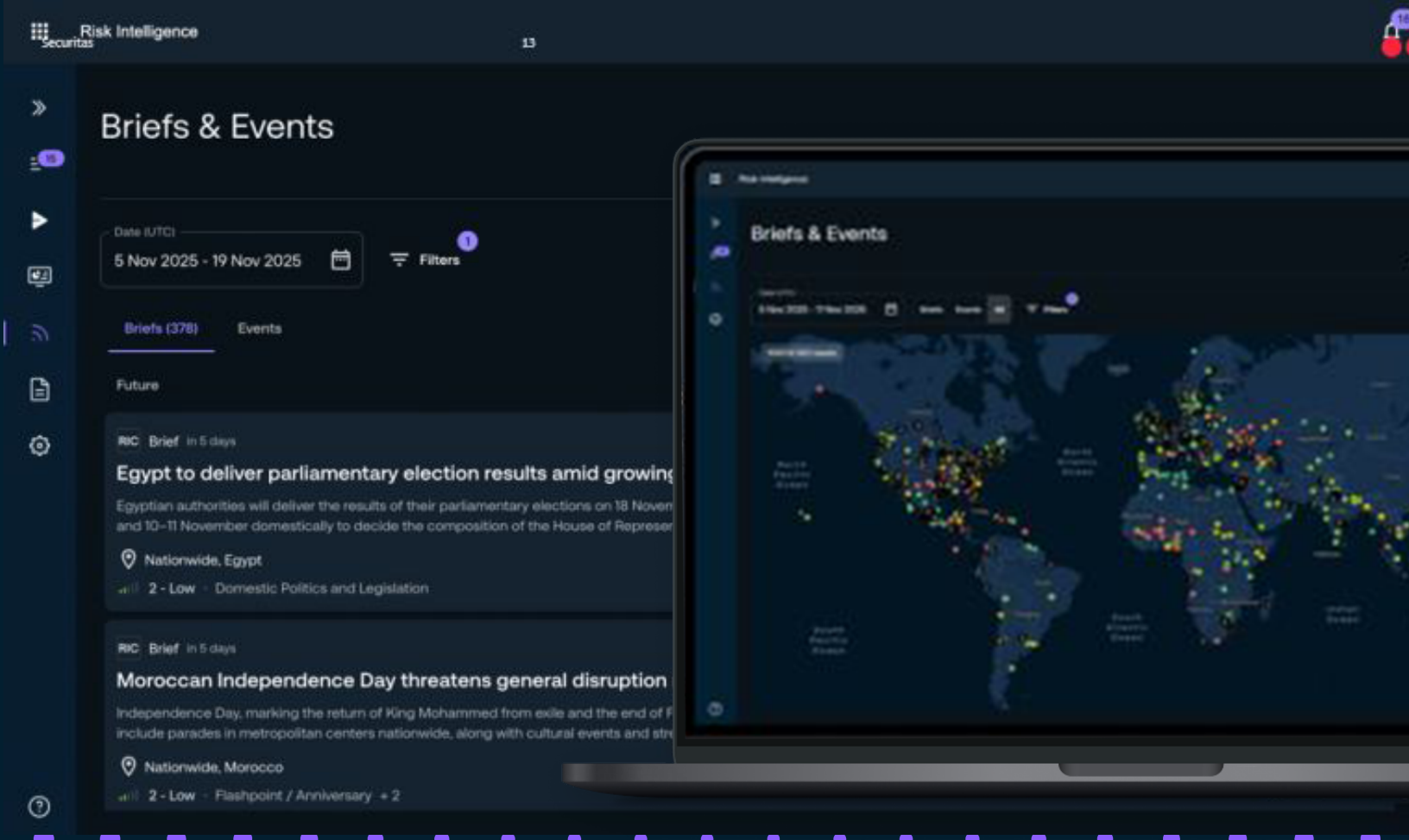
- AI tools (including free-to-access large language models such as ChatGPT, Gemini and Grok) can be utilized to search for personally-identifiable information (PII) on targets, and if privacy guardrails are not implemented (or bypassed) can potentially return accurate details including contact numbers, family names and home addresses.
- The aftermath of the assassination of Charlie Kirk highlights the increasing use of social media for the identification of targets for retaliatory actions such as coordinated harassment, doxxing, and real-world intimidation by actors seeking to exploit heightened public sentiment.
- Ongoing socio-political polarization alongside an increase in actual or perceived economic insecurity will likely fuel growing discontent and negative sentiment towards specific organizations. This will highly likely lead to an associated increase in targeting of CEOs and executives as the 'public face' of the company.
- Differing privacy and data protection laws will make continue to make consistent enforcement and regulation challenging, potentially driving governments to consider restrictions or limitations on social media platforms.

Scenario	Scenario condition	Assessed likelihood
An improving geopolitical and socio-political outlook drives a decrease in CNI targeting, chiefly due to reduced activist desire and intent. Nations reduce the use of proxy actors to conduct GZW actions as tensions ease.	Improves	Highly unlikely (20%)
Global tensions continue to rise, centered around ongoing conflicts and flashpoints, including environmental, social, and economic (ESG) issues; activists increasingly target CNI to increase exposure for their causes.	Baseline	Likely / Probable (55%)
Geopolitical tensions escalate further, driving more nation-states to engage in increasingly direct targeting of CNI, including deployment of proxy assets as part of wider attack methodologies.	Worsens	Unlikely (25%)

Advisory

- Ensure that regular audits of publicly available personal information are conducted for organization executives, and remove any details that could be exploited.
- Monitor social media to detect any changes in online sentiment that may result in organizational executives being targeted.
- Ensure that incident response plans are in place and regularly practiced to effectively address incidents of doxing, safeguarding organizational executives and business sites.

Indicators	Implications
— Social media platforms being identified as having weak or inconsistent content moderation. — Increasing polarization of social media platforms, with platforms becoming ‘echo chambers’. — An increase in digital activism and use of social media for delivering ‘social justice’. — Rise in general harassment and targeting of organizations and individuals within social media platforms. — Increased use of bot networks and algorithm-driven systems to present and distribute mis / dis / malinformation. — Publishing of databases of CEO’s and other executives, particularly for organizations subject to increased public scrutiny and discontent	— Organizational executives face significant risks to personal safety if targeted through a mass doxxing campaign. — Rising concerns over the facilitation of doxxing campaigns through social media may lead to stricter regulations and compliance requirements for social media sites, particularly in areas such as data privacy. — Organizations may be required to invest in crisis management resources to monitor, identify, and respond to instances of doxxing of executive members.


Risk Intelligence
Briefs & Events
Date (UTC)
5 Nov 2025 - 19 Nov 2025
Filters
Briefs (378)
Events
Future
RIC Brief in 5 days
Egypt to deliver parliamentary election results amid growing
Egyptian authorities will deliver the results of their parliamentary elections on 18 Noven
and 10–11 November domestically to decide the composition of the House of Represer
Nationwide, Egypt
2 - Low · Domestic Politics and Legislation
RIC Brief in 5 days
Moroccan Independence Day threatens general disruption
Independence Day, marking the return of King Mohammed from exile and the end of F
include parades in metropolitan centers nationwide, along with cultural events and str
Nationwide, Morocco
2 - Low · Flashpoint / Anniversary + 2

Global

Shared socioeconomic grievances drive further spread of ‘Gen Z’ protest movements

Large-scale anti-government protests primarily conducted by youth populations under the ‘Gen Z’ banner emerged in multiple countries, including Algeria, Madagascar, Mexico, Nepal, and Peru in 2025, with protesters denouncing poor economic conditions, political instability, and governmental corruption. The high-profile successes of some of these groups, involving the instigation of regime change in certain cases, in conjunction with shared socioeconomic factors, are expected to encourage the spread and intensification of such protest actions throughout 2026.

- It is highly likely that countries across the Global South will continue to be particularly affected by future protests, due to the regions’ having conditions conducive to student / youth unrest prompted by economic and political grievances.
- Violent confrontations between protesters and local authorities are highly likely to result in nationwide disruptions and represent a threat to official buildings and organizations with perceived connections with the government. Band waving, slogans, and the extensive use of youth symbols will highly likely be exploited to attract further participants to join the demonstrations.
- The use of social media will almost certainly remain a definitive characteristic of ‘Gen Z’ protests, enabling the movements to communicate and coordinate actions in a decentralized manner, exacerbating nationwide disruptions and compromising response from local authorities.

Scenario	Scenario condition	Assessed likelihood
The ‘Gen Z’ trend slows down, but protests continue to occur with less violence and clashes reported with law enforcement.	Improves	Unlikely (10%)
Protests continue to spread and attract further participation, resulting in major changes in the political landscape without necessarily meeting the entirety of protesters’ grievances.	Baseline	Likely / Probable (40%)
The success of previous ‘Gen Z’ demonstrations encourages the formation of new groups. Violent protests spread globally and exacerbate insecurity in regions already experiencing instability.	Worsens	Likely / Probable (45%)

Advisory

- Enhance monitoring of online platforms used by ‘Gen Z’ movements to coordinate their activities, including Discord, Facebook, Instagram, LinkedIn, Reddit, TikTok, and X.
- Security teams are advised to implement emergency response plans and strengthen security protocols to maintain business operations and ensure the safety of their assets and personnel. The implementation of contingency should address flexible work arrangements, such as remote work.
- Organizations should maintain clear communication with consulates and embassies to stay informed about the situation’s development and assess the business environment’s safety.

Indicators	Implications
— ‘Gen Z’ groups continue to mobilize on social media globally, with large-scale protests planned and promoted in advance. — Large ‘Gen Z’ protest movements result in significant political change. — Heightened security measures are mobilized by political leaders, particularly in the surroundings of official buildings. — The current unrest landscape in the affected country is elevated, with protesters from diverse backgrounds denouncing socio-economic policies. — Backlash and online criticisms towards the government increase.	— Due to the large attendance and TTPs used, ‘Gen Z’ protests are expected to disrupt business operations and local supply chains. — Major political change will result in the amendment of legislation for businesses operating in the affected country. — Increased security measures for organizations located in protest-prone areas will result in high financial costs. — Violent clashes with local authorities will result in property / infrastructure damage and jeopardize the safety of assets for organizations located in protest-prone areas.

US economic policy sustains global uncertainty and risk

Global market instability will persist through 2026 due to unpredictable US economic policies, causing impacts across multiple industries, particularly those perceived to be driving trade imbalance, including steel / aluminium, automotives, electronics / technology, clothing, rare earth metals, food and agriculture, and pharmaceuticals. A pending Supreme Court case on the Trump administration's use of the International Emergency Economic Powers Act is likely to reduce its ability to set arbitrary restrictions; however, in this case, efforts to apply targeted, albeit limited levies through interpretations of the 1974 Trade Act or 1962 Trade Expansion Act remain a realistic possibility.

- Whilst the use of direct military action remains remote, US rhetoric in 2025 signalled US consideration of military operations to exert influence on strategically significant locations (such as Greenland or the Panama Canal) in response to perceived geoeconomic threats posed by adversaries.
- Indications that the US is considering the use of force or otherwise exerting pressure on non-adversaries to enhance its strategic position will induce significant negative market sentiment and alienate existing US allies.
- Organizations seeking to mitigate uncertainty may create further market instability through measures such as stockpiling, near- / off-shoring, and reviewing logistics and supply chain relationships. Approaches such as increased digitization and centralization carry their own risks, such as increased exposure to cybersecurity threats.

Scenario	Scenario condition	Assessed likelihood
US continues targeted restrictions with court-enforced limits, which sustains negative market sentiment, albeit with more predictable and narrow targets.	Improves	Likely / Probable (55%)
US continues to enact restrictions in an unpredictable and arbitrary manner, such as punishing political disagreements with trade partners, driving US allies to explore alternative trading partners to ensure procurement of key goods.	Baseline	Realistic possibility (40%)
US conducts military operations to seize control of strategic economic chokepoints, worsening global economic instability and regional security.	Worsens	Remote (5%)

Advisory

- Consider developing escalation plans to guide decision-making amid rapidly shifting regulations, with consideration for operational continuity in affected regions.
- Audit / introduce loss prevention and mitigation strategies, particularly for organizations with global supply chains.
- Organizations involved in supply chain logistics should consider reviewing impacts to operations based on the loss of services provided by US-centric companies (including AI and GPS-based systems).

Indicators	Implications
— The Supreme Court delivers a ruling in early 2026 limiting Executive authority in setting tariffs and export controls. — The White House directs the Commerce Secretary to conduct investigations under the Trade Expansion Act. — Increasing political rhetoric from US administration around taking / controlling key strategic areas. — Bilateral deals between US allies (e.g., Western Europe, Canada) deepen with China and middle powers (e.g., Colombia). — AI-enabled market solutions seeking to address supply chain challenges problems rapidly emerge.	— Fluctuations in costs impact business financial forecasts and valuation. — Markets become increasingly opportunistic or unviable, causing business operation relocation. — Increased expenditure to mitigate security vulnerabilities due to new / unfamiliar processes and protocols. — US policy causes specific industries or organizations to suffer financial loss due to compliance violations. — Businesses experience pronounced insider threat, particularly if they deal in critical industries.

Proliferation of terror materials on open-source platforms drives self-initiated terror threat

Extremist content, terrorist manifestos, and ideological propaganda will continue to proliferate online throughout 2026, including on mainstream social media, gaming platforms, and decentralized file-sharing sites. This content will enable self-initiated terrorists (S-ITs) - individuals with no formal links to established terrorist groups - to plan and conduct attacks with little to no external support. Easy access to detailed guidance on attack planning and target selection in conjunction with the availability of emerging technologies such as drones and 3D printers will drive ongoing shifts in the physical security threat landscape.

- S-ITs will almost certainly remain the most difficult threat vector for security services to effectively monitor, given their lack of ties to established networks and minimal digital footprints. S-ITs often replicate tactics, techniques, and procedures (TTPs) available in openly circulating manuals, particularly low-complexity attacks such as vehicle rammings, melee weapon and small-arms assaults.
- The increasing politicization and fragmentation of social media platforms, combined with the inability for content moderation to keep pace, will create ideal conditions for social media users to self-radicalize.
- Extremist groups are already experimenting with the use of generative AI tools, indicating the potential for exploitation in the medium to long term. AI will highly likely be used to circumvent existing content moderation systems and exploit crises through the rapid creation and dissemination of propaganda to incite violence.

Scenario	Scenario condition	Assessed likelihood
The spread of openly accessible extremist material decreases due to improved content moderation, slowing the path to self-radicalization and forcing potential extremists into established (and monitored) pathways.	Improves	Highly unlikely (10%)
S-IT attacks persist at current levels as extremist content remains accessible across public platforms, allowing individuals to radicalize independently.	Baseline	Likely / Probable (55%)
The volume and sophistication of publicly accessible terrorist materials significantly increases, driving a surge in self-initiated plots globally.	Worsens	Unlikely (35%)

Advisory

- Develop scenario plans for common terrorist attack types, including attack scenarios involving melee weapons, explosives, firearms, fire as a weapon, vehicles as weapons, kidnap-ransom-extortion (KRE), and harmful substances, including chemical, biological, radiological, and nuclear (CBRN).
- Ensure that staff are aware of the signs of and processes for reporting potentially radicalized individuals and provide training and tools to facilitate and support employees.
- Implement monitoring and alerting processes for identifying and verifying potential threat incidents through on the ground-personnel, local news and social media, corroborating any information with official / credible sources.

Indicators	Implications
— National security agencies issue alerts / raise terror levels warning of rising self-initiated threats linked to online radicalization. — Expansion of propaganda content targeting previously untapped regional or demographic groups (i.e., propaganda translated into different languages). — Substantial increase in shares, downloads, or reposts of extremist manuals and propaganda across open-source platforms. — Tech platforms disbanding content moderation teams or changing their policies, allowing more extremist content to go unchecked.	— Organizations in major metropolitan areas experience operational disruptions due to elevated threat levels and increased security measures. — Target profile for S-ITs widens as online extremist content interacts with personal grievances, with potential targets including private organizations. — Companies become more likely to experience reputational harm and potential regulatory action if their services, platforms, or products are exploited to produce, host, or distribute terror materials.

AMEA

Middle East security landscape complexifies following Gaza ceasefire

Major developments in the Middle East continued to exacerbate region-wide uncertainty in 2025, compounded by the collapse of the first Gaza-Israel ceasefire in March; the 12-day Iran-Israel conflict in June; and the cessation of nuclear negotiations between Iran and the US. While a second ceasefire in Gaza has been in place since October, tensions in the Middle East remain heightened, with little resolution in sight for many of the key drivers of regional tension as 2026 begins.

— As the US and other states seek to establish an international task force in Gaza to support post-conflict governance and stability, it is likely Israel will express opposition to the involvement of certain states, namely Türkiye, preserving disagreements over the territory's future administration.

— After suffering considerable losses during direct and proxy conflicts with Israel in 2025, Iran and its proxy groups will likely seek to regenerate and refresh capability, with the aim of returning to previous strategic goals and tactics. Whilst widespread influence is likely to be challenging in 2026 due to the scale of losses, attacks on key strategic and ideological targets (such as actions on the Yemeni border) will almost certainly persist.

— Iranian-US nuclear talks remain stalled, with little sign of progress. With no immediate path to an agreement being apparent, bilateral tensions will almost certainly remain elevated throughout 2026, maintaining risks to Western assets from Iranian gray-zone warfare (GZW) operations such as cyber attacks.

Scenario	Scenario condition	Assessed likelihood
A long-term peace agreement in Gaza is established. Improved Israel / US relations with Iran / Syria lead to formal security arrangements, de-escalating the security landscape.	Improves	Highly unlikely (10%)
Little progress in Iran-US nuclear negotiations, with isolated clashes in the Middle East region (Gaza, Lebanon, Syria) threatening renewed kinetic conflict and further uncertainty.	Baseline	Realistic possibility (50%)
Renewed kinetic conflict in separate theaters involving Israel (Gaza, Iran, Lebanon, Syria), resulting in renewed targeting of maritime shipping in the Red Sea, disrupting commercial operations.	Worsens	Realistic possibility (40%)

Advisory

— Develop detailed business continuity plans that account for various disruption scenarios, including maritime route closures, regional banking disruptions, and supply chain interruptions at the local, regional, and global levels.

— Review and enhance cyber security measures to protect against state-sponsored attacks, particularly focusing on critical infrastructure and sensitive data.

— Maintain awareness of the potential for Middle East tensions to continue to motivate threat actors internationally, including activists and terrorists / extremists.

Indicators	Implications
— Increase in incidents in Gaza / Lebanon involving Israeli military forces and Iranian proxies such as Hamas / Hezbollah. — Sharp increase in maritime security incidents in the Red Sea and Persian Gulf, particularly involving vessels linked to Israeli or Western interests. — Sudden shifts in Israeli troop movements and / or deployments in Gaza, Lebanon, and Syria. — Breakdowns in talks over international task force in Gaza and its post-conflict governance. — Escalations in Israeli tensions with Syria / Iran, including increased rhetoric around Gaza.	— Rapid shifts in regional dynamics as a result of changing allegiances, such as US relations with Israel / Syria. — Renewed disruption to regional supply chains and shipping routes, particularly affecting energy and maritime sectors. — Growth in frequency / intensification of activities by the global pro-Palestine movement, posing threats to Western organizations with real / perceived links to Israel. — Strategic shift required in business operations due to regional developments creating new security dynamics.

Islamist militants expand activity in West Africa

Various Islamist groups, including Boko Haram and the Islamic State West Africa Province, continued to escalate attacks across the Sahel and West Africa in 2025, targeting civilians, military personnel, government institutions, and business assets. Countries such as Burkina Faso, Niger, and Mali will continue to feel the impacts of the withdrawal of Western military support for counterterrorism operations. Mali will likely continue to experience the most pronounced escalation, driven by the growing influence of Jama'at Nusrat ul-Islam wa al-Muslimin (JNIM), which has disrupted fuel supply chains between Senegal and the Malian capital, Bamako in late 2025.

- Affected states are likely to face growing international isolation, as foreign governments issue travel advisories to protect nationals. This is highly likely to exacerbate economic challenges, slow investment and growth, and further entrench extremist groups, particularly in remote areas, where counterterrorism efforts remain insufficient.
- Islamist groups, particularly JNIM, are likely to increasingly conduct transnational operations, exploiting areas with weak government control to launch attacks across borders and potentially abroad. These efforts will likely be further enhanced by the groups' growing use of advanced technologies, such as drones, to carry out attacks.
- Attacks on foreign investments, mining operations, and critical infrastructure are likely to escalate, potentially including coordinated extortion campaigns, kidnapping-for-ransom operations, and deliberate disruptions of regional supply chains linking landlocked Sahel states to coastal ports.

Scenario	Scenario condition	Assessed likelihood
Regional states, together with international partners, launch region-wide counterterrorism operations, driving groups into increasingly remote areas.	Improves	Highly unlikely (10%)
Islamist groups continue to launch attacks; however, they remain domestic threats within individual countries or confined geographical areas. Regions remain hostile to foreign nationals and businesses.	Baseline	Realistic possibility (40%)
Islamist groups continue to escalate and expand attacks across borders, posing increasing threats to political stability / foreign assets, and interests throughout the region.	Worsens	Realistic possibility (50%)

Advisory

- Monitor government advisories and public statements, including restrictions to specific regions and sub-regions, security deployments, and safety precautions such as shelter-in-place advisories.
- For companies operating in volatile regions, implement robust security and personnel protection measures, as well as contingency measures / continuity plans in the event of targeting.
- Develop and maintain communication plans with personnel in volatile regions to ensure swift reporting of advisories and shifts in security arrangements.

Indicators

- Attacks increase in frequency and severity, increasingly targeting larger population areas.
- Attacks begin to occur in previously unaffected regions / states.
- Kidnapping, ransom, and extortion of foreign nationals increases.
- Rise in mobility restrictions and supply chain disruptions attributed to extremist groups.
- Regional governments organize meetings to plan coordinated counterterrorism actions.
- Further foreign government travel advisories that also begin to include neighboring nations.

Implications

- Domestic unrest escalates in affected regions, leading to protests and violent clashes in urban areas.
- Critical supply chains of minerals from the regions are disrupted, impacting the operations of dependent sectors.
- Humanitarian challenges escalate in affected regions, including famine, disease outbreaks, and restricted access to critical aid supplies.
- Foreign nationals face increased security threats, with risks extended to expatriates, diplomatic staff and business personnel.

Reemerging markets present opportunity and risk to businesses

The alleviation or cessation of conflicts across the AMEA region throughout 2025 has opened up opportunities for renewed private sector involvement. Syria's reintegration into the international community / global economy under the new regime of President Ahmed al-Sharaa marks the most significant example; however, the ongoing ceasefire in Gaza, less intense fighting / a limited ceasefire in Myanmar, the disarmament of the Kurdistan Worker's Party (PKK), and peace agreements in the Democratic Republic of Congo (DRC) and between Armenia and Azerbaijan are also likely to present opportunities in 2026.

— Access to previously inaccessible markets and lucrative reconstruction and development contracts is likely to encourage foreign direct investment (FDI), which, alongside foreign state aid, sanctions being removed, and human capital returning from abroad, has the potential to improve humanitarian conditions and drive economic growth.

— Despite conflicts de-escalating, the security situation remains fragile in many cases. Risks include former combatants turning to criminality or conducting revenge attacks to undermine authorities, lingering sociopolitical tensions hindering development and reconstruction efforts, or conflict re-escalating in response to a flashpoint.

Scenario	Scenario condition	Assessed likelihood
Rapid economic improvement in post-conflict countries is propelled by positive reconciliation among previously competing factions and significant financial support from international partners.	Improves	Highly unlikely (10%)
Ceasefire / conflict cessation holds with moderate levels of residual security issues. Economic rebuilding proceeds gradually but is tempered by lingering tensions.	Baseline	Realistic possibility (50%)
Conflict re-erupts, with new competing factions among the ruling regime taking up arms, or previous rivals choosing to return to conflict or engage in violent insurgency.	Worsens	Realistic possibility (40%)

Advisory

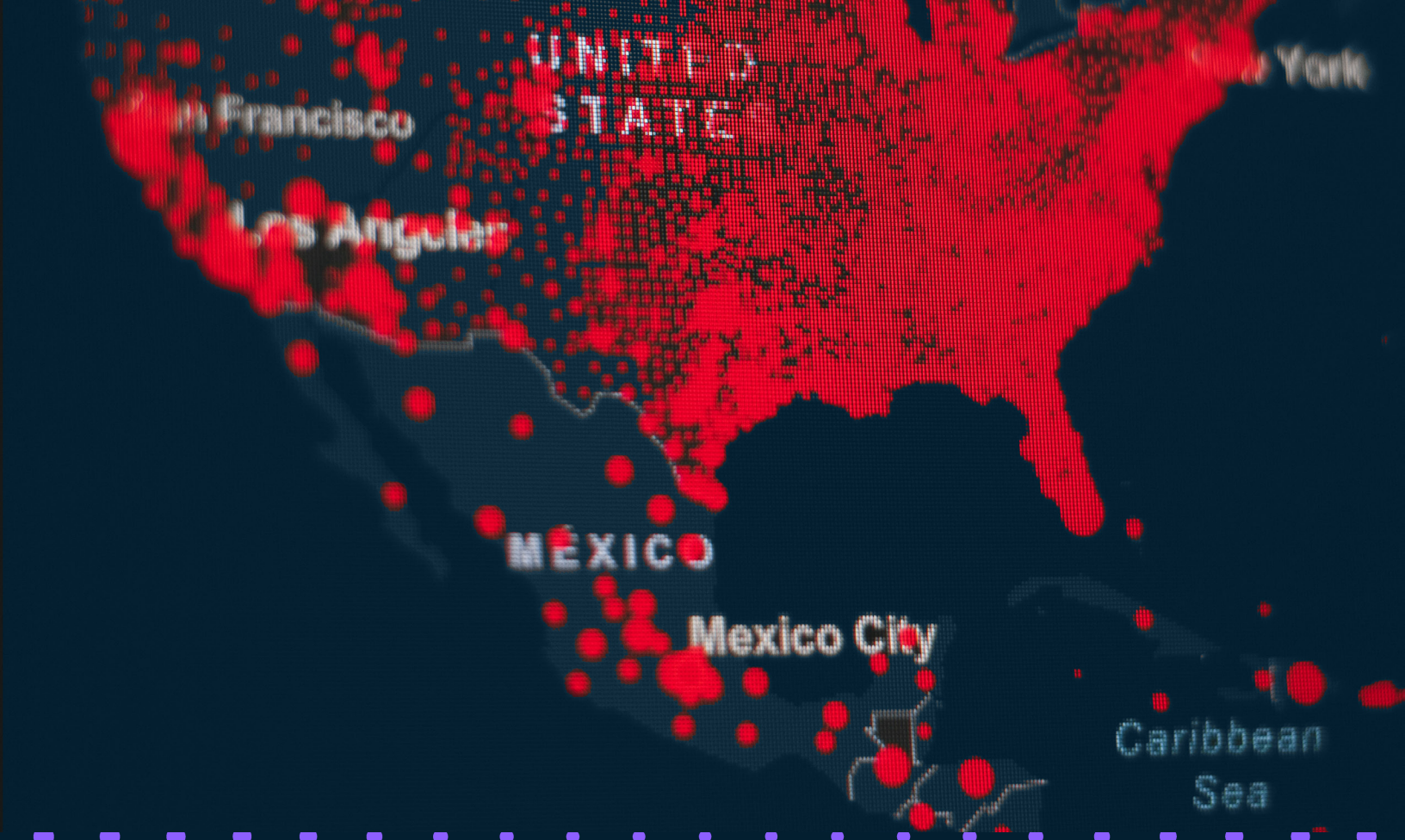
— Companies considering engaging in reopening markets should conduct rigorous due diligence and risk assessments for conducting business in the country and create robust contingency plans for a range of potential security issues.

— Hire vetted and trusted local nationals to navigate the complexities of the post-conflict state. These should include both individuals who remained in the country during the conflict, refugees who fled the fighting, and dual nationals familiar with the language and culture of both the host nation and the involved company.

— Invest in multilayered and appropriate security measures, including trusted local personnel, in-house physical security and intelligence staff, and established channels with key figures including peacekeeping forces and embassy attaches.

Indicators	Implications
— Sustained involvement of key geopolitical blocs in negotiations between parties engaged in conflict. — Formal reestablishment of diplomatic relations and reopening of embassies by major states. — Suspension and / or easing of sanctions and tariffs for countries involved in conflict. — Organizations expanding operations into areas previously impacted by conflict. — Increased rate of returning refugees to impacted countries.	— The reintegration of multiple countries / areas into the global economy is likely to shift supply chains and present lucrative economic opportunities. — Organizations that heavily invest in reemerging markets are highly likely to face significant exposure in the event conflict resumes or the security situation becomes destabilized. — Businesses that closely cooperate with new authorities or a single faction risk being viewed as a legitimate target in residual fighting. — Reverse migration trends will potentially lead to new tensions over issues such as land ownership.


STANDARD



Americas

US reorientation to Latin America exacerbates political uncertainty and regional instability

The US's reorientation of its foreign policy towards Latin America (LATAM) following Donald Trump's return to the presidency is expected to continue in 2026. The approach was initially aimed at countering organized crime groups' (OCGs) drug trafficking operations, but has since evolved to reasserting US influence over the region, acting as a significant driver of political uncertainty and regional instability. The US's renewed involvement in the region is highly likely a reaction to growing concerns over China's increasing political and economic influence in LATAM.

- The US launched airstrikes on ground targets in Venezuela and apprehended President Nicolas Maduro during an operation in the early hours of 3 January. US President Donald has since indicated the US will oversee a transition of power in the country and has threatened further action if national authorities do not cooperate; however, transition plans have not been publicly disclosed in detail, and the situation remains volatile.
- The recommissioning / modernizing of US military facilities in the Caribbean has the potential to facilitate long-term deployment of sophisticated military assets. LATAM countries are highly likely to perceive this as a security threat, potentially leading to strengthening economic and military ties with US strategic rivals.
- The US is likely to escalate gray-zone warfare (GZW) operations in LATAM, particularly in countries perceived to be 'unfriendly' toward the US. The Trump administration has demonstrated its willingness to force regime change and use inflammatory rhetoric to influence foreign politics is almost certain to increase political division in LATAM.

Scenario	Scenario condition	Assessed likelihood
The US cooperates with national authorities to oversee a peaceful and orderly transition of power in Venezuela and reduces its military buildup around the Caribbean Sea.	Improves	Highly unlikely (10%)
The situation in Venezuela continues to be unstable and volatile as details surrounding a US-led transition of power remain unclear. Simultaneously, the US continues pressure regimes in countries such as Colombia and Cuba.	Baseline	Likely / Probable (65%)
Venezuela's security landscape deteriorates as competing factions seek to assert authority over the country, while the US takes further action against the leadership of adversarial regimes.	Worsens	Unlikely (25%)

Advisory

- Assess exposure / reliance on specific regions' supply chains / trade routes, aiming to diversify and minimize disruptions caused by geopolitical events.
- Develop contingency plans for disrupted diplomatic relations, heightened periods of threat / unrest, and invest in geopolitical risk intelligence services to monitor, anticipate, and respond to developing conflicts.
- Develop detailed business continuity plans that account for various disruption scenarios, including maritime route closures, regional banking disruptions, and supply chain interruption, for businesses in the region and internationally.

Indicators	Implications
— Ongoing renewal and refurbishment of US military infrastructure in the Caribbean, such as airbases and naval facilities. with additional deployments of sophisticated hardware to the region. — Increased anti-US messaging from various LATAM countries and vice versa from the US. — Demonstrations in LATAM countries, citing 'US imperialism,' demanding cessation of US interference in domestic affairs and severing of ties with the US. — Announcements of increased cooperation / agreements between LATAM states with US strategic rivals. — Shifts in US policy choice to undertake direct action in certain LATAM countries.	— Increased compliance complexity for multinational corporations operating across LATAM and US jurisdictions. — Increased protest landscape / direct action targeting of US-linked organizations by pro-LATAM / anti-US activist groups, adversely impacting organization operations. — Regional uncertainty undermines investor confidence, reducing foreign investment. — Deterioration of diplomatic relations, even between long-term allies, resulting in obstructions to employees' travel and bilateral trade.

Political extremism growing in scope and frequency in the US

Acts of political extremism have increased significantly in the US in the past two years, driven by the widening of existing political divisions, and the increased prevalence of and access to far-left / right political views across US society. Increasingly unmoderated and partisan social media environments are leading to individuals are becoming increasingly self / externally radicalized, and with the current administration showing no signs of walking back its more divisive policies and rhetoric, further acts of politically motivated extremism in 2026 are highly likely.

— The use of Immigration and Customs Enforcement (ICE) and other agencies to crack down on illegal immigration, cuts to federal departments, and economic impacts from global trade tariffs will continue to drive political polarization. Activist and extremist groups will highly likely continue to focus on these topics and those promoting, implementing or supporting them.

— Nationwide 'days of action' in opposition to government policy will likely continue, providing flashpoints and platforms for potential political extremism from both anti-Trump protesters and counter-protesters.

— Extreme actions such as assassinations and acts of sabotage, violence and serious vandalism will almost certainly continue to be planned, driven by both inflammatory rhetoric and highly divisive policymaking and the increasing normalization of extreme viewpoints in both mainstream and alternative media.

Scenario	Scenario condition	Assessed likelihood
US reorientation into LATAM improves regional stability, strengthening US economic and geopolitical ties to the region. While also diminishing US strategic rivals' influence / market access, particularly in rare earth minerals.	Improves	Remote (5%)
US interference raises regional tensions with LATAM states, harming the US's international image, while largely being ineffective at countering US strategic rivals' strategic objectives.	Baseline	Likely / Probable (70%)
LATAM states opposition to US interference results in regional instability, enabling exploitation by US strategic rivals and state and non-state backed threat actors.	Worsens	Unlikely (25%)

Advisory

— Maintain awareness of the protest landscape and demonstrations that could act as a platform for political extremism, particularly during periods of increased political activity, such as the 2026 midterm elections.

— Consider reviewing portfolios to identify any elements that could be perceived as being connected to a political party / group / policy and could be targeted by extremist actors.

— Organizations are advised to maintain a strong understanding of trends regarding the tactics, techniques, and procedures (TTPs) of political extremists who successfully or planned to carry out threat actions.

Indicators	Implications
— Political figures within mainstream politics continue to vocalize and disseminate extremist rhetoric. — An elevated protest landscape persists with symbolic events, such as federal holidays, acting as flashpoints for unrest. — Controversial or divisive policies are enacted or reinforced despite political and public backlash. — The Trump administration implements measures to guard federal assets against political violence. — Activist groups are designated as 'terrorist organizations', with the designation being used to facilitate law enforcement action.	— Organizations with perceived links to political initiatives suffer security threats related to political extremism. — Increasing political polarization and radicalization will heighten the risk of insider threat incidents, particularly in organizations close to divisive topics. — Foreign confidence in the US business landscape will likely degrade while political extremism remains high. — Foreign adversaries are highly likely to exploit the normalization of political extremism to direct it at businesses in strategically important sectors.

US shifts approach from ‘War on Terror’ to ‘War on Crime’

The Trump administration has shifted US military operations from counterterrorism toward counter-crime in the latter months of 2025. Continuation or escalation of this approach is highly likely through early 2026. Where previously, the US military adopted a counterinsurgency approach with the war on terror, the Trump administration is increasingly using terrorist designations to target criminal groups and those perceived to be adversarial to US government goals. This includes designating several drug cartels in Latin America as foreign terrorist organizations (FTOs), as well as foreign and domestic left-wing groups / philosophies, including Antifa in the US and Antifa Ost in Germany.

- The designation of foreign and domestic criminal groups as FTOs allows the Trump administration to alter its approach when targeting these groups, enabling the use of military capabilities against strategic targets.
- While the Trump administration has demonstrated its intent to invest resources into countering crime in the US, this has led to an increase in strikes on foreign organized crime groups, many of which are now FTOs, as well as an increase in crackdowns on opposition protest groups. Both give the US access to increased capabilities to target foreign adversaries deemed complicit in criminal activity, including foreign governments.
- Trump will likely continue to attempt to employ the US National Guard supplement crime-fighting and law enforcement capabilities in cities across the US. If these deployments escalate into domestic / international strikes, it would highly likely trigger legal and constitutional challenges.

Scenario	Scenario condition	Assessed likelihood
The US government scales back the use of terrorist designations to target criminal and activist groups. While some criminal groups are designated as FTOs, US military activity remains limited.	Improves	Highly unlikely (10%)
The Trump administration continues to designate foreign criminal groups as FTOs to facilitate the use of military forces against domestic groups designated as such.	Baseline	Likely / Probable (70%)
Widespread criminalization of opposition groups and activists leads to the deployment of military assets domestically and internationally, promoting unrest and legal challenges.	Worsens	Unlikely (20%)

Advisory

- Assess exposure / reliance on specific regions’ supply chains / trade routes, aiming to diversify and minimize disruptions caused by geopolitical events.
- Develop contingency plans for disrupted diplomatic relations, heightened periods of threat / unrest, and invest in geopolitical risk intelligence services to monitor, anticipate, and respond to developing conflicts.
- Maintain awareness of domestic and foreign political relations, as US political and the Trump administration’s relationship can impact both the domestic and foreign trade environment.

Indicators

- Continued designation of foreign criminal groups as FTOs, giving precedent for the US government to implement similar designations on domestic groups.
- The Trump administration continues to use the National Guard to counter anti-government protests, releasing narratives calling for the criminalization of left-wing activist groups.
- Increasingly inflammatory rhetoric between Republican and Democratic politicians that leads to further scapegoating for domestic challenges.
- Violent attacks conducted by foreign criminal organizations are being perceived as terrorist activity, allowing the government to implement designations.

Implications

- An increasingly restrictive social environment, where political opposition is increasingly criminalized.
- Organizations with operations abroad will be increasingly impacted by negative sentiments toward the US government.
- Foreign criminal groups, those with FTO designations, will become increasingly violent and radical, potentially leading to implications for businesses worldwide.
- US pressure on foreign governments to adhere to FTO designations and combat domestic criminal activity from left-wing groups, leading to political uncertainty in affected countries.


NETHERLANDS
Amsterdam
Rotterdam
Hanover
Bielefeld
GERMANY
Essen
Dusseldorf
Cologne
Antwerp
Brussels
BELGIUM
Lille
English Channel
London
Frankfurt am Main
Nuremberg
Mannheim
Luxembourg
Saarbrucken
Stuttgart
Paris

Europe

5

Civilian recruitment alters the threat landscape across Europe

Hostile actors are increasingly leveraging civilians, both unwittingly and deliberately, to advance their strategic objectives in European states, altering the traditional profile of threat actors and complicating attribution and protective measures for governments and businesses. China has been accused of using its nationals and coerced individuals to conduct espionage against sensitive sites; Russia has reportedly recruited individuals to carry out criminal acts such as arson or to operate drones targeting critical national infrastructure (CNI), while Iran has been accused of employing French and Swedish organized crime groups (OCGs) and funding pro-Palestine groups to further its interests abroad.

— The increasing use of civilians by threat actors is likely fueled by efforts to dismantle traditional espionage networks across the West amid heightened geopolitical tensions, which is highly likely to persist into 2026 and beyond if tensions remain elevated.

— This trend will likely lead to an increase in hostile reconnaissance, sabotage, and targeted attacks that will be increasingly difficult for authorities to detect or prevent, necessitating enhanced surveillance capabilities and protective measures, while remote recruitment methods provide operational security for threat actors.

— Although this approach complicates attribution, it will almost certainly intensify geopolitical tensions and heighten suspicion in Western states toward foreign nationals from adversarial countries. There is also a realistic possibility that this suspicion will extend to businesses, which are also vulnerable to coercion or exploitation.

Scenario	Scenario condition	Assessed likelihood
Enhanced surveillance and counterintelligence reduce incidents and improve attribution. Suspicion toward foreign nationals is managed, and operations / attacks are less frequent.	Improves	Unlikely (25%)
Hostile actors continue using civilians at current levels, with Incidents occurring sporadically but remaining manageable.	Baseline	Unlikely (25%)
Hostile actors increasingly exploit civilians resulting in an increase in attacks. Attribution becomes increasingly difficult, and businesses face higher operational and security risks.	Worsens	Likely / Probable (55%)

Advisory

— Enhance threat detection and security protocols at sensitive sites, including strengthened cyber security measures, surveillance, employee vetting, and access controls.

— Implement and maintain comprehensive staff training on social engineering, coercion risks, and recognizing suspicious behavior, while promoting clear reporting channels for potential insider threats.

— Monitor adversarial state activities and emerging recruitment tactics, including propaganda campaigns, and stay updated on regulatory and compliance requirements related to civilian-targeted threats.

Indicators	Implications
— Increase in sabotage / espionage incidents targeting sensitive government / business sites. — Increase in targeted attacks against dissident communities / communities viewed as hostile to adversarial states. — Online content increasingly targets civilians with propaganda / recruitment, especially on encrypted platforms. — Increase in civilian arrests with reported evidence of links to state actors, including those without ideological motivation. — An increase in low-sophistication attacks, including the increased use of readily accessible civilian drone technology to disrupt critical infrastructure / conduct hostile reconnaissance.	— Disruptions to critical infrastructure, supply chains, and business continuity become more frequent and harder to prevent. — Businesses face increased security and compliance costs and a heightened threat of insider incidents. — Reputational risks grow due to leaks of sensitive information and perceptions of weak security. — Heightened tensions following incidents between states disrupt economic ties and lead to measures against foreign businesses from adversarial countries, impeding their operations and market access.

Anti-migration sentiments elevate across Europe

Rising levels of irregular migration in Europe have triggered significant public backlash, fueling stronger anti-migrant sentiment across the region, a trend likely to intensify through 2026. This shift has been accompanied by an uptick in right-wing rhetoric, with many right-wing groups framing increased migration as a central political issue. As a result, several European governments are adopting policies aimed at addressing irregular migration, further fragmenting both public opinion and political discourse.

— Right-wing / far-right groups will likely continue to organize protests to exert pressure on European governments to address irregular migration, particularly if migration figures continue to increase.

— Increasing political polarization and the rise of alternative media are likely to increase the potential for opposing groups to engage in hostile actions. Organized protests are likely to result in counterdemonstrations, increasing the risk of clashes between opposing groups and / or security forces.

— Anti-migration protests will continue to be promoted and attended by high-profile figures, driving increased attendance. and are likely to garner additional momentum when in response to incidents allegedly involving migrants, particularly where these crimes are violent and / or sexual in nature. These tensions have the potential to be inflamed by acts of information disorder from hostile nation-states and threat actor groups.

Scenario	Scenario condition	Assessed likelihood
The frequency and intensity of migration-related violence and unrest decrease as governments address associated concerns.	Improves	Highly unlikely (15%)
Anti-migration protests and unrest continue to escalate across Europe, with alleged criminal activity associated with migrants acting as flashpoints for high-profile demonstrations.	Baseline	Realistic possibility (45%)
Increase in violent rhetoric following high-profile crimes involving migrants, prompting anti-immigration groups to form more formal and sophisticated networks to coordinate joint actions.	Worsens	Realistic possibility (40%)

Advisory

— Maintain awareness of planned protests near business assets, and develop response plans to manage scenarios, including enhancing security measures at sites and implementing strategies to minimize operational disruptions.

— Coordinate with local law enforcement when large demonstrations are anticipated near business assets.

— Avoid public-facing messaging that associates the organization with political positions, particularly if migration related.

— Maintain awareness of the political calendar and the potential for unrest to occur as a result.

Indicators	Implications
— Heightened protest landscape in European states affected by increased irregular migration, influenced by anti-migration sentiments. — Attempts to reform border controls and asylum-related policies fail to deter large numbers of irregular migrants from entering Europe. — Right-wing / far-right groups continue to gain electoral support, driven in part by their firm stance on irregular migration. — Governments introduce policies and regulations, including restrictions on protests and increased punishments, to curtail disruptive and harmful actions.	— Large-scale protests and clashes with security forces are likely to disrupt transportation routes, employee mobility, and supply chains. — Demonstrations near an organization's operations are likely to increase the risk of incidental exposure to violence or property damage. — Employees from migrant backgrounds face potential elevated safety risks, harassment, or discrimination in or around protest-affected areas. — Escalating social tensions are likely to complicate stakeholder engagement for organizations in Europe, particularly for businesses in politically sensitive sectors.

European governments under financial pressure amid economic transition

Numerous European countries are facing mounting fiscal pressure as a result of high state spending, demographic trends, and geopolitical / geoeconomic challenges, posing a risk to the region's long-term economic outlook and social cohesion. Political and economic tensions between European countries and China, in conjunction with announced plans to further decouple from Russia's natural resources and other emerging trends such as the rise in protectionist economic policies and the US' erratic economic policy, make this trend likely to extend into 2026 and beyond.

— Planned measures to reduce France's fiscal deficit and national debt have been significant drivers of political instability and social unrest throughout 2025, with multiple mass demonstrations and strike actions involving hundreds of thousands of participants taking place throughout September and October. It is probable the implementation of similar austerity measures in other European countries will act as a flashpoint for unrest.

— The European Commission is considering issuing individualized reforms to member states as part of a plan to tie pension reforms to central funding in the 2028 budget to lower the fiscal risk posed by the bloc's aging population, according to reports from 17 October.

— EU member states are required to submit national diversification plans, detailing how they intend to eliminate direct and indirect imports of Russian oil and gas by 1 March 2026, while other sanctions will come into force throughout the year.

Scenario	Scenario condition	Assessed likelihood
An improving geopolitical and socio-political outlook drives a decrease in CNI targeting, chiefly due to reduced activist desire and intent. Nations reduce the use of proxy actors to conduct GZW actions as tensions ease.	Improves	Highly unlikely (10%)
Global tensions continue to rise, centered around ongoing conflicts and flashpoints, including environmental, social, and economic (ESG) issues; activists increasingly target CNI to increase exposure for their causes.	Baseline	Likely / Probable (55%)
Geopolitical tensions escalate further, driving more nation-states to engage in increasingly direct targeting of CNI, including deployment of proxy assets as part of wider attack methodologies.	Worsens	Unlikely (35%)

Advisory

— Evaluate the likelihood of current business operations, contracts, or partnerships being adversely affected by planned or future austerity measures, and assess their exposure.

— Integrate macroeconomic and geopolitical indicators into regular risk monitoring and proactively monitor to identify signals of instability driven by supply chain disruptions and policy changes.

— Diversify supply chains to more stable legal jurisdictions and incorporate Environmental, Social, and Governance (ESG), political, and credit risk metrics into supplier selection and monitoring.

Indicators	Implications
— The EU instructing member states to take further action against fiscal deficits and high levels of national debt. — Countries taking financial deficit reduction measures, such as retirement age changes, cutting welfare programs, and degrading pension programs. — The economic relationship between European countries and the US deteriorates at short notice, likely as a result of a political dispute. — Countries failing to approve annual budgets. — China announces new probes involving industries associated with European trade or against specific European importers.	— Economic conditions will almost certainly have a significant influence on the region's political landscape, with deterioration encouraging support for radical / fringe parties. — Austerity measures and other fiscal reforms shape the region's business landscape and affect long-term planning. — Increasingly frequent or potentially intense labor union protest / strike action in countries across the region. — Increased probability of mass layoffs and job losses occurring across a range of industries.


Intelligence Reports
Risk Intelligence Center
Daily Global Intelligence Report – 28 September
Summary

Wild cards

Global markets destabilized by AI bubble burst

The growing valuation of companies associated with Artificial Intelligence (AI) has raised growing concerns that the industry is in a bubble, with many drawing parallels to the dot-com bubble that emerged around the new millennium and led to a severe market crash. The 'Magnificent Seven,' namely Alphabet, Amazon, Apple, Meta, Microsoft, Nvidia, and Tesla, have a combined market cap of ~$21.5 trillion, representing ~35% of the total market capitalization as of November 2025, and have continued to see rising investment despite these concerns, largely due to the increased productivity and projected economic growth that AI technology promises.

— Nvidia, a fundamental actor, has a market value of ~$5 trillion, greater than the GDP of Japan, meaning small valuation shifts, caused by events such as missed earnings calls or regulatory changes, have the potential to cause significant market swings in global markets.

— Investors have flagged that many 'hyperscale' companies spread the cost of graphic processing units (GPU) over ~five to six years despite Nvidia releasing new architectures that depreciate the value of previous generations much faster, in a practice described as one of "the more common frauds of the modern era."

— Industry valuation has been driven in part by spending commitments made by several companies that are significantly higher than their current annual revenue. OpenAI's revenue is estimated at ~$20 billion in 2025, but it has committed to invest ~$1.4 trillion into companies such as AWS, Microsoft, and Oracle between 2025-2032.

Scenario	Scenario condition	Assessed likelihood
Organizations slow borrowing to fund AI development, resulting in a less concentrated market capitalization, decreased volatility around the influence of AI, and helping to avoid a bubble 'burst'.	Improves	Unlikely (15%)
The speculative bubble continues to grow and exacerbates pressure on financial markets, resulting in more risk, volatility, and uncertainty.	Baseline	Realistic possibility (40%)
The valuation of AI-associated companies continues to grow without any major technological breakthroughs or significantly increased revenue streams, leading to an eventual market crash.	Worsens	Realistic possibility (40%)

Advisory

— Upskill workforces to mitigate market volatility and ensure long-term resilience by developing human skills such as ethical reasoning and complex problem-solving.

— Diversify asset portfolios with other technologies focused on improving operational capabilities, mitigating the operational impact of loss of access or significant cost increases to AI capability.

— Maintain awareness of fluctuating AI market signals and financial regulatory changes to inform contingency plans that mitigate the threat of collapse.

Indicators	Implications
— Reduced confidence observed among tech organizations and investors. — Valuations continue to rise and result in a new, sustained market focused on technology. — Organizations from the ‘Magnificent Seven’ miss earnings / sales targets, increasing market volatility. — AI-associated organizations engage in mass layoffs or adopt other cost-cutting measures. — Economic conditions worsen, resulting in higher interest rates. — Organizations ask governments for an economic bailout or protection to ensure their sustainability.	— Economic recession negatively affects gross domestic product (GDP), employment rates, living standards, and savings plans. — Future technological development will be delayed due to a possible widespread loss of trust in sophisticated technologies. — Public unrest stemming from heightened anti-sentiments against AI and the financial sector. — Tightened financial regulations driven by political and public pressure to prevent future crashes.

Elevated geopolitical competition in the Arctic region

Competition for control of access to resources, shipping routes, and strategic territory in the Arctic is rising, as global warming-driven ice melt makes the region more accessible. This has led to increasing militarization of the Arctic and raised tensions between competing countries. Wider global tensions – particularly between Russia, the US and northern European countries – will likely accelerate the race to claim and control key routes and locations in the region in 2026.

- Global powers, such as Russia and the US, are increasingly competing for control of the Arctic, primarily through investing in technologies intended to improve regional access and project influence such as icebreaker vessels, with both countries seeking to expand access to and usage of new potential shipping routes.
- NATO members are conducting joint military exercises in the Arctic with increasing frequency, while those with Arctic territory, such as the Nordics, have developed partnerships with members lacking Arctic territory to boost security in response to Russian efforts to develop military presence in the region.
- Territorial disputes, largely over areas believed to host critical minerals and other natural resources, are reportedly being prioritised above the concerns of indigenous populations, underlining the ineffectiveness of regional institutions, such as the Arctic Council, regarding their ability to protect the rights of the region's inhabitants.

Scenario	Scenario condition	Assessed likelihood
Efforts to identify viable shipping routes are unsuccessful or deemed non-viable, decreasing interest in the Arctic. Countries with interests in the region identify routes to cooperation, such as through agreements on limits to military or industrial presence.	Improves	Highly unlikely (10%)
Militarization of the Arctic continues to increase steadily, while Russian gray-zone warfare (GZW) actions become more frequent. Competition for territory is driven by discovery of large reserves of natural resources or strategically significant locations.	Baseline	Likely / Probable (65%)
Russia reduces focus on Ukraine (either due to ceasefire or a shift in strategy), switching efforts toward increasing its influence in the Arctic region, raising the risk of military confrontation.	Worsens	Unlikely (25%)

Advisory

- Businesses with interests in the Arctic or Nordic regions – including supply chains such as shipping routes - are advised to maintain a awareness regarding geopolitical developments in the region.
- Prepare contingency plans due to the potential for armed confrontations and military disputes to take place in the Arctic, including the closure or restriction of key trade routes.
- Organizations with links to operations related to global interest and development in Arctic territories should assess the potential for backlash and negative reputational impacts associated with criticism from indigenous populations.

Indicators	Implications
— Credible scientific bodies and studies indicate Arctic ice melt is continuing or increasing. — Countries and alliances with interests in the Arctic region purchase or build assets likely to be used to expand or solidify their presence (such as icebreaker ships). — NATO and Russian military exercises in the Arctic grow in frequency and scale. — Russian GZW actions targeting regional competitors increase in frequency and complexity. — Indigenous communities in the Arctic elevate efforts to raise awareness of their grievances and protest the actions of regional competitors.	— Organizations operating in the Arctic, particularly those in strategic industries, will likely be at risk of targeting by GZW threat actions such as sabotage. — Legal disputes over contested territories are likely to cause challenges for businesses operating in the region. — Organizations with interests in the Arctic become targets for activism related to indigenous populations. — Militarization and potential escalations are likely to incite investor concerns and divestment from certain Arctic assets. — Improved infrastructure along Arctic shipping routes is likely to strengthen dependent supply chains.

Space domain elevates threat to national security and private sectors

Increasing dependence on space-based technology – and associated efforts by nation-states to exert influence and control over space - will likely accelerate national security and commercial threats in 2026. Russia, China, and the US notably advanced space-based military capabilities in 2025, including anti-satellite (ASAT) systems and counter-missile deployments. While space-based weapons architecture is a longer-term aspiration, the threat of impacts to communications and geolocation networks from both natural phenomena and human intervention, such as grey-zone warfare (GZW) targeting satellites, will likely continue to rise.

- Commercial satellites will highly likely factor into military and GZW planning, risking disruptions to systems providing key services such as communications, satellite imagery, and navigation / geolocation services.
- Additionally, increasing dependence on highly sensitive technology is almost certain to expose organizations to the risk of impacts associated with phenomena such as solar radiation, including outages and system damage. The next solar maximum, expected in early 2026, will serve as a potential trigger for solar flares and coronal mass ejections, which in turn increase the risk of downtime to key power and communications infrastructure.
- An international agreement regulating the development of military or potentially hostile space-based technology is unlikely, increasing the risk of a space 'arms race' and associated threats such as GZW actions.

Scenario	Scenario condition	Assessed likelihood
Major powers develop a binding dialogue on limiting space-based offensive capability, while the 2026 solar maximum passes with minimal impacts.	Improves	Unlikely (10%)
Nations continue to proliferate space-based capabilities, employing GZW with attempts at disrupting CNI, while solar radiation contributes to isolated disruptive events.	Baseline	Likely / Probable (70%)
Global / mass infrastructure failure event occurs due to major loss of satellite capability, whether due to direct military intervention, GZW actions or extreme space weather events.	Worsens	Highly unlikely (10%)

Advisory

- Assess exposure to impacts associated with a loss of systems dependent on satellite technology, in particular connectivity (both telephony and internet), geolocation and tracking, and imagery.
- Review any dependencies on equipment sensitive to spikes in solar radiation and the impacts associated with downtime or damage to the above.
- Consider conducting tabletop exercises or 'wargaming' for scenarios such as a major geomagnetic storm and the associated impacts.

Indicators

- US Space Force operationalizes combat systems as anticipated; China and Russia deploy space and terrestrial ASAT tools.
- Increasing geopolitical tensions over deployment or development of space-based technologies (including weapons).
- Increases in disruptions reported by services reliant on satellite technology.
- Ground terminals associated with satellite functionality report surge of cyberattack intrusion attempts.
- Solar pulse activity occurs in line with previous solar maximum events, including several solar flares of coronal mass ejections.

Implications

- Navigational / GPS system outages result in shipment and transportation delays.
- Digital system failures potentially halt global payment transfers, driving financial uncertainty.
- Loss of access to satellites linked to critical national infrastructure (CNI) severely degrades emergency services and telecommunications.
- Disruption to surveillance enables military operations, worsening regional security.
- Early warning systems for severe weather events and natural disasters become ineffective, hindering evacuation and continuity planning.

Flashpoints and significant dates

2026 Flashpoints and significant dates AMEA

JAN

- **1 Jan**: Taiwanese Republic Day
- **3 Jan:** Anniversary of Qasem Soleimani assassination
- **14 Jan:** Anniversary of Tunisian Revolution
- **15 Jan:** Anniversary of the 2024 Ra'anana terrorist attack
- **25 Jan**: Anniversary of the 2011 Egyptian Revolution

FEB

- **1 Feb:** Anniversary of the 2021 Myanmar military coup
- **11 Feb:** Islamic Revolution Day (Iran)
- **14 Feb:** Anniversary of the 2011 Bahrain uprising
- **15 Feb:** Afghan Liberation Day
- **15 Feb:** Anniversary of the 2011 Libyan Revolution
- **20 Feb:** Anniversary of the 2011 Moroccan reform protests

MAR

- **5 March:** Nepalese general elections
- **15 March:** Anniversary of the 2019 Christchurch Mosque shooting
- **17 March:** St Patrick's Day
- **28 March:** Al Quds Day
- **30 March:** Eid al-Fitr

APR

- **1-9 April:** Passover
- **5 April:** Easter Sunday
- **14 April:** Yom HaShoah

MAY

- **1 May:** May Day
- **7-10 May:** India-Pakistan conflict anniversary
- **15 May:** Al Nakba Day
- **25 May:** Jerusalem Day

JUN

- **1 June:** Ethiopian general elections
- **4 June:** Anniversary of the 1989 Tiananmen Square massacre
- **4 June:** Hajj Pilgrimage
- **13-24 June:** Anniversary of the Iran-Israel conflict
- **26 June:** Ashura

JUL

— **24-28 Jul:** Cambodia-Thailand border dispute anniversary

AUG

— **14 August:** Pakistani Independence Day
— **15 August:** Indian Independence Day

SEP

— **21 Sept:** Yom Kippur
— **25 Sept:** Sukkot

OCT

— **7 Oct:** Third anniversary of the Gaza-Israel conflict escalation
— **9-19 Oct:** Anniversary of Afghanistan–Pakistan conflict
— **14 Oct:** Anniversary of the Malagasy coup d'état

NOV

— **2 Nov:** Balfour Day
— **8 Nov:** Diwali
— **30 Nov:** Kyrgyz parliamentary elections

DEC

— **5 Dec:** Gambian presidential elections
— **5-12 Dec:** Hanukkah
— **11 Dec:** Anniversary of 1948 UN General Assembly Resolution 194
— **22 Dec:** South Sudan holds its first general election
— **25 Dec:** Christmas
— **31 Dec:** New Year's Eve

2026 Flashpoints and significant dates

Americas

JAN

- **1 Jan:** New Year's Day
- **6 Jan**: Anniversary of US Capitol Hill insurrection
- **7 Jan:** Anniversary of the Juliaca massacre
- **11-17 Jan:** Al-Aqsa week
- **27 Jan:** Holocaust Memorial Day
- **27 Jan:** Isra and Miraj

FEB

- **4 Feb:** Anniversary of the 1992 Venezuela coup attempt
- **13-14 Feb:** Shab-e-Barat
- **13-18 Feb:** Rio Carnival
- **14 Feb:** Anniversary of 2024 Kansas City parade shooting
- **17 Feb:** US Presidents' Day
- **26 Feb:** Maha Shivrati

MAR

- **17 March:** St Patrick's Day
- **28 March:** Al Quds Day
- **30 March:** Eid al-Fitr

APR

- **1-9 April:** Passover
- **5 April:** Easter Sunday
- **12 April:** Peruvian general election

MAY

- **1 May:** May Day
- **5 May:** Cinco de Mayo
- **15 May:** Al Nakba Day

JUN

- **26 June:** Ashura

JUL

— **4 July:** US Independence Day

AUG

— **6 Aug:** Bolivian Independence Day
— **30 Aug:** Haiti General Election

SEP

— **10 Sept:** First anniversary of the assassination of Charlie Kirk
— **20-27 Sept:** Climate Week NYC 2026

OCT

— **4 Oct:** Brazilian general elections
— **7 Oct:** Third anniversary of the Gaza-Israel conflict escalation

NOV

— **2 Nov:** Balfour Day
— **3 Nov:** US midterm elections
— **8 Nov:** Diwali

DEC

— **5-12 Dec:** Hanukkah
— **11 Dec:** Anniversary of 1948 UN General Assembly Resolution 194
— **25 Dec:** Christmas
— **31 Dec:** New Year's Eve

2026 Flashpoints and significant dates Europe

JAN

- **1 Jan:** New Year's Day
- **7 Jan**: Anniversary of 2015 Charlie Hebdo terror attack
- **19-23 Jan:** World Economic Forum
- **11-17 Jan:** Al-Aqsa week
- **27 Jan:** Holocaust Memorial Day
- **27 Jan:** Isra and Miraj

FEB

- **13 Feb:** Munich Security Conference
- **13 Feb:** 2025 Munich car attack anniversary
- **13-14 Feb:** Shab-e-Barat
- **24 Feb:** Anniversary of the 2022 Russian invasion of Ukraine
- **28 Feb:** Anniversary of the Tempe Train Disaster

MAR

- **17 March:** St Patrick's Day
- **28 March:** Al Quds Day
- **30 March:** Eid al-Fitr

APR

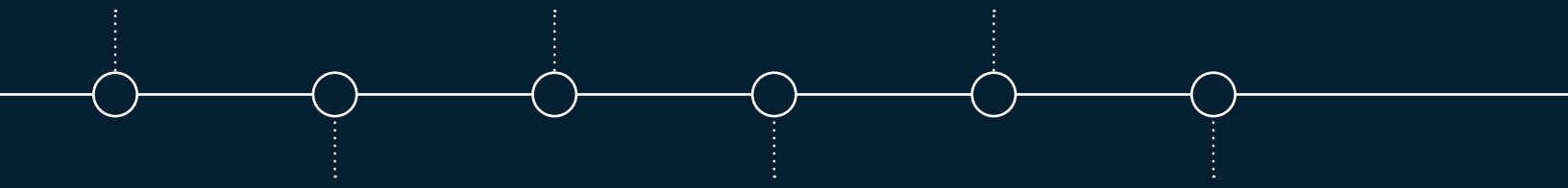
- **1-9 April:** Passover
- **3 April:** Hungarian parliamentary elections
- **5 April:** Easter Sunday

MAY

- **1 May:** May Day
- **9 May:** Victory Day
- **15 May:** Al Nakba Day

JUN

- **7 June:** Armenian general elections
- **26 June:** Ashura



JUL

— **14 July:** Bastille Day

AUG

— **24 August:** Ukrainian Independence Day

SEP

— **13 Sept:** Swedish general elections

OCT

— **3 Oct:** Latvian parliamentary elections
— **7 Oct:** Third anniversary of the Gaza-Israel conflict escalation

NOV

— **2 Nov:** Balfour Day
— **8 Nov:** Diwali

DEC

— **5-12 Dec:** Hanukkah
— **11 Dec:** Anniversary of 1948 UN General Assembly Resolution 194
— **25 Dec:** Christmas
— **31 Dec:** New Year's Eve

Contact

intelligence@securitas.com