Securitas

Securitas Risk Intelligence

Clarity in a noisy world

Annual Intelligence Estimate 2026 Mid-Year Review

As Sophie Cairney, Lead Risk Intelligence Consultant, Securitas Risk Intelligence Center, notes: “The 2026 risk landscape is defined less by isolated threats and more by convergence. Organizations are operating in an environment where geopolitical, technological, and societal risks intersect and influence one another. The challenge is not only responding to disruption, but recognizing the early indicators of change.”

Contents

Introduction

OPERATING IN A RISK-DEFINED ENVIRONMENT

The first six months of 2026 have reinforced a clear reality for organizations: risk is no longer a background consideration; it is a central force shaping strategic decision-making and a defining feature of today's operating environment. At mid-year, the security and threat landscape remains defined by uncertainty rather than stability. The key differentiator is preparedness. Organizations best positioned for the remainder of 2026 are those that treat risk as a strategic input, using intelligence to protect their people, property, and assets.

Through continuous intelligence monitoring and analysis, Securitas Risk Intelligence has observed a sustained shift in how risk evolves and impacts organizations. Risk is no longer isolated; it is persistent, interconnected, and increasingly decisive in shaping operational and strategic decision-making and outcomes. Daily intelligence reporting highlights that geopolitical instability, technological disruption, and security threats are not only more frequent but also more interlinked and impactful than ever before.

This Mid-Year Review reflects an environment of constant disruption, but also the ability to anticipate and adapt by using situational awareness and specific intelligence. Each section of the Annual Intelligence Estimate has been updated, providing a timely assessment of emerging risks, their impact on business operations, and how our Risk Intelligence Center (RIC) analysts expect them to continue evolving.

KEY THEMES FROM H1 2026

RIC analysis indicates that threat actors continue to evolve in both intent and capability. We are seeing inreased targeting of critical national infrastructure and high-value corporate assets, including people and physical sites. Intelligence reporting highlights a growing use of blended tactics, combining cyber activity, physical targeting, and information manipulation - to maximize disruption and enforce longer-lasting impacts on organizations' security, operations, and reputation.

At the same time, the rapid adoption of artificial intelligence is emerging as a consistent feature across threat vectors, enabler of threat activity, including disinformation and social engineering, and as a source of new organizational vulnerabilities, particularly linked to insider risk. The information threat landscape is becoming more contested, with a growing volume of misinformation and weaponized online content complicating situational awareness and increasing reputational threats.

Across political and economic environments, volatility remains high. Domestic unrest, shifting geopolitical alliances, and regional instability contribute to uncertainty in policy direction and operating conditions worldwide. This is reflected in increased reporting on supply chain disruption, regulatory divergence, and market instability. Alongside this, we observe sustained growth in activism and grievance-driven movements, with digital platforms accelerating the speed at which local issues can escalate into broader disruptive events.

The ability to anticipate, prioritise, and act decisively will define organizations' security in the months and years ahead.

Sophie Cairney
Lead Risk Intelligence Consultant

Team Members

Matthew Phillips
Global Intelligence Team Lead

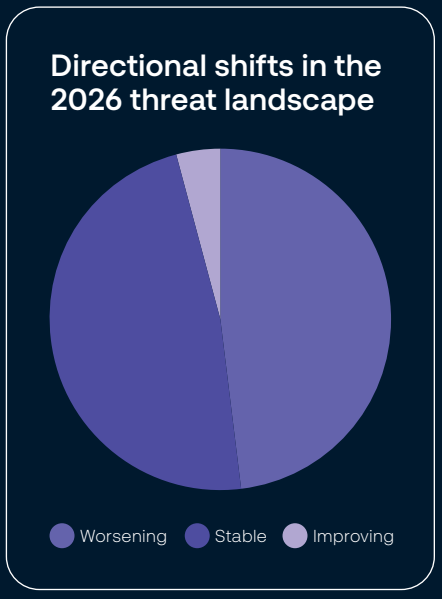
Jessica Wilson
Risk Intelligence Analyst

Alma Abraham
Risk Intelligence Analyst

John Coudriet
Intelligence Analyst (Embedded)

Clarity in a Noisy World – Annual Intelligence Estimate Mid-Year Review is developed by Securitas' Risk Intelligence Center (RIC), the operating unit within Securitas Risk Intelligence.
The RIC continuously monitors geopolitical developments, emerging threats, and industry specific risk patterns, transforming complex information into clear, evidence based intelligence that underpins Securitas Risk Intelligence assessments and advisory services.

Methodology



The Annual Intelligence Estimate 2026

Published in January, the Annual Intelligence Estimate 2026 provided thematic assessments of key commercial and geopolitical risk vectors, providing actionable intelligence for corporate security and risk professionals.

The estimate offers cross industry situational understanding, through an accessible, strategic summary supported by practical guidance. It bridges strategic risk assessment for senior leadership with the tactical intelligence required by operational teams and facilitates the consideration of current risk vectors to enable the implementation of proportionate and effective security precautions to protect people, infrastructure, and operations.

Mid-Year Review

The Mid-Year Review reevaluates these assessments, using evolving, diverging, and adapting trends to provide an updated view of the 2026 landscape aligned with the featured topics of the Annual Intelligence Estimate.

Each topic is revisited with an overview of the current situation, two focussed assessments relevant to awareness and corporate security, and supporting evidence drawn from activities during Q1 & Q2 2026. Advisory considerations are included to support business security decision-making.

In this year's mid-year review, 12 of the 25 assessment topics worsen, 12 stabilize, and one improve, as depicted in the chart to the left.

Our intelligence-led approach

Assessments are produced by RIC, using open-source intelligence and subject-matter expertise across corporate security and the global threat landscape, with particular focus on the convergence of the two.

Since the first Annual Intelligence Estimate in 2023, several themes, such as AI, supply-chain vulnerabilities, information disorder, geopolitical conflict and ESG-related backlash, have remained prominent. While the threat landscape continues to evolve, these themes highlight the volatility of corporate security and the importance of an intelligence-led posture.

The graph below illustrates how assessed situations have shifted over time relative to their threat levels, demonstrating that the two do not always directly correlate; a worsening situation may not raise the threat to corporate security, whereas a stabilized situation may continue to present a consistently high threat.

Threat level vs. Situational change

X: Degree of Situational Change

Y: Threat Level to Corporate Security

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

Safeguard your organization with industry-leading intelligence. Securitas Risk Intelligence goes beyond identifying what is happening. It also explains why it matters, what could happen next, and, most importantly, what actions can be taken. With four levels of premium services, we offer digital tools, managed services, and embedded expertise, all combined to create a tailored solution that meets your unique needs. In addition we offer Ad-hoc Intelligence and consultancy to meet our clients specific needs.

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.

Corporate security

1

Threat actors continue to favor targeting CNI to maximize disruption

The outbreak of the Iran conflict on 28 February highlighted the significant threats posed to critical national infrastructure (CNI), such as airports, data centers, utilities facilities, and energy infrastructure, in the event of conflict, and the increasing capability / willingness of both state and non-state threat actors to attack such targets. Targeting throughout the conflict has largely been enabled by technological developments associated with, and the widespread adoption of, one-way attack unmanned aerial vehicles (OWA-UAVs), with attackers seeking to maximize economic impact and disruption to public life. Attacks conducted in the cyber domain have also played a notable role.

Outside of armed conflict, threat actors have continued to target CNI as part of gray-zone warfare (GZW) operations and activist campaigns. While national authorities across the globe and intergovernmental organizations continue to announce and implement measures aimed at increasing the security of CNI, low-sophistication tactics, techniques, and procedures (TTPs) are still capable of causing significant disruption and can often be challenging to attribute if appropriate operational security (OPSEC) precautions are taken.

- Threat actors are highly likely to escalate targeting of CNI in 2026, particularly during high-tension geopolitical flashpoints and if states increasingly view CNI as legitimate targets in the event of conflict and alter their military posture to reflect this. While investment and regulatory reforms aimed at protecting CNI will almost certainly continue, such infrastructure is highly likely to remain vulnerable to a range of TTPs.
- The persistent targeting of CNIs throughout 2026 is highly likely to incite organizations to implement additional physical security measures, particularly during heightened tensions for regions at greater risk from proxy threat actors, potentially incurring additional costs. However, digital threats such as disinformation campaigns and cyber attacks are highly likely to increase with limited possibility for protective measures.

Significant developments

Date	Location	Description
1 May	London, US	Pro-Iranian hacktivist group, the Islamic Cyber Resistance in Iraq, also known as 313 Team, claimed responsibility for the 503 errors Ubuntu's website experienced as a result of a DDoS attack, announcing via a Telegram post that the attack was scheduled to persist for four hours.
6-7 Apr	Central France	Coordinated sabotage attacks in Bourges, La Chapelle-Saint-Ursin, and Saint-Florent-sur-Cher, France, targeted power grid infrastructure supplying French defense manufacturers KNDS and MBDA, causing localized outages that disrupted arms production activity.
15 Mar	Dubai, UAE	The Dubai Civil Aviation Authority ordered a temporary suspension of operations at Dubai International Airport after an Iranian drone strike caused a fire near the airport.
4 Jan	Berlin, Germany	Left-wing extremist group, Vulkangruppe, claimed responsibility for an arson attack in Berlin, Germany, which caused widespread power outages.

Advisory

- Assess CNIs vulnerabilities considering threats to the industry it comes under and the specific location, and consider additional physical security and cybersecurity measures.
- Maintain awareness of localized and geopolitical tensions that are pre-action indicators for CNI targeting.
- Ensure strong contingency plans are prepared to secure supply chains and maintain operational capacity of CNI sites.

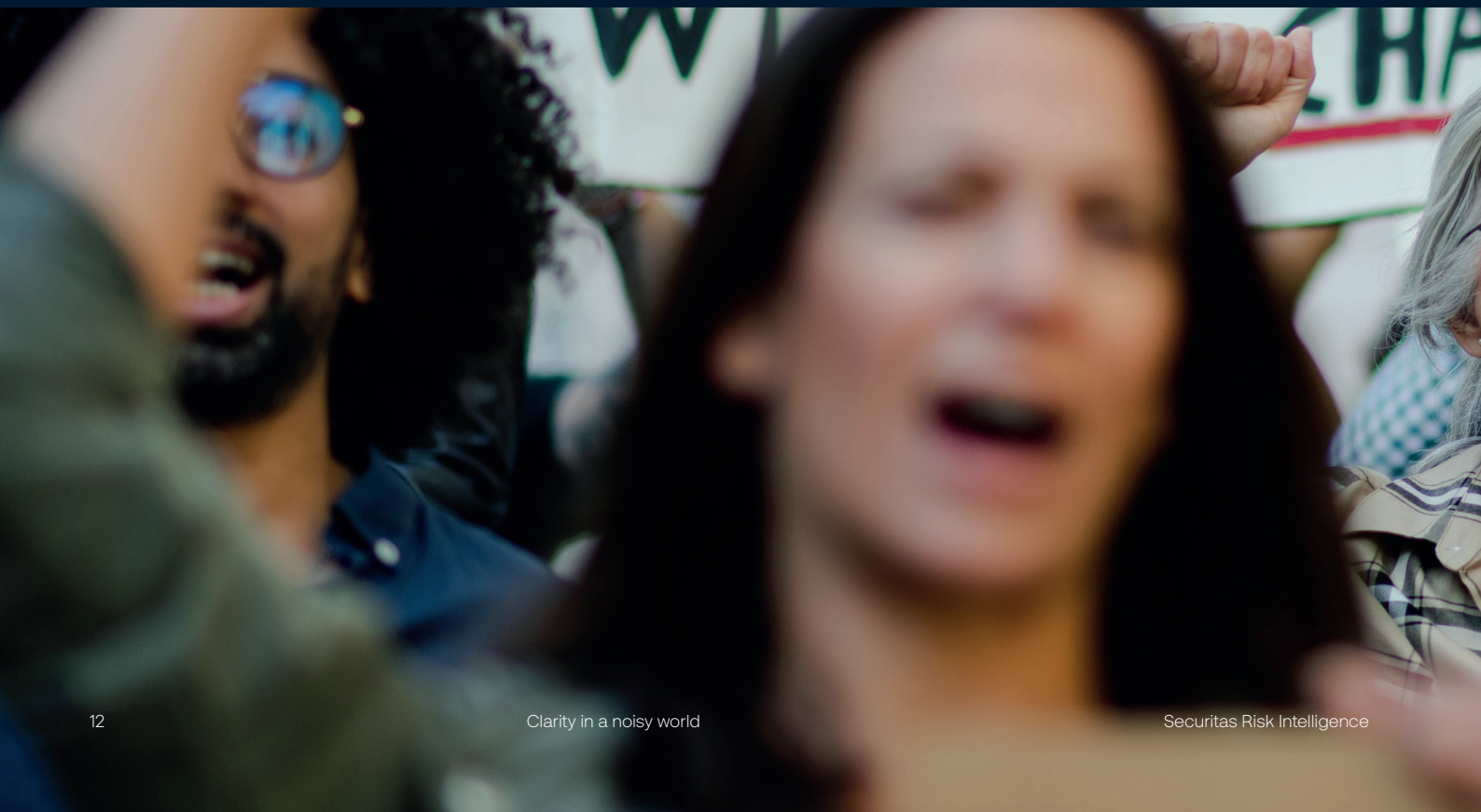
Backsliding corporate progress on ESG challenges drives activism

Organizations perceived to be violating environmental, social, and governance (ESG) policies, such as diversity, equity, and inclusion (DEI) initiatives, continue to be targeted by activist groups through online / in-person boycotts, demonstrations at company sites, and online scrutiny in 2026. Backsliding is being encouraged by measures implemented by the US government to reduce the prevalence of DEI initiatives and increase economic conditions under President Donald Trump, and the loosening of environmental regulations in the EU. Company events such as annual general meetings and major escalations related to geopolitical conflicts and / or governance developments serve as regular flashpoints for activism. Activist groups use a variety of tactics, techniques, and procedures (TTPs), ranging from peaceful protests outside site locations to more direct-action TTPs such as vandalism and criminal damage of sites and assets, aiming to pose substantial operational disruptions.

Activists are increasingly using open-source information to identify organizations' positions on polarizing / controversial issues and affiliations with states / entities they deem problematic, including identifying whether existing ESG schemes have been adhered to and / or whether companies remain committed to divestment statements.

- Activist groups are highly likely to develop evolved direct-action TTPs to pose high levels of disruption at industry events and company locations with high-profile visitors, as well as conduct criminal damage at late-night / early-morning hours to evade detection. Protesters are also likely to target second / third party organizations to pose greater impacts on the target organization's supply chains and investment strategies.

- Organizations accused of backsliding on ESG commitments are likely to experience heightened threat from activism, leading to a shift from in-person hosted events to online platforms. Although this is likely to reduce physical targeting of events, it is unlikely to deter activists from protesting events, and rather, protests are likely to shift toward digital actions.



Significant developments

Date	Location	Description
7 Apr	Adelaide, Australia	Activists with Weapons Out (WO) protested at BAE Systems' site in Adelaide, Australia, over the company's role in supplying F-35 jet components and connections to military action in Gaza.
17 Feb	Orlando, US	Activists from the Rainforest Action Network (RAN) disrupted Mondelēz International CEO Dirk Van de Put's plenary address at the Consumer Analyst Group of New York (CAGNY) conference in Orlando, Florida, to pressure the company on weak deforestation and human rights protections in its global supply chains.
29 Jan	Amsterdam, Netherlands	Fossil Free Netherlands demonstrated outside the 'Leaders in Sustainable Finance' event at the Pakhuis de Zwijger cultural center in Amsterdam, to protest BlackRock's perceived hypocrisy and investments in fossil fuels.

Advisory

- Maintain confidentiality of communications regarding policy changes to reduce leaks that are likely to be exploited by activists.
- Consider the potential of insider risk in the period after policy changes have been announced by monitoring employee sentiment regarding changes.
- Maintain situational awareness of evolving TTPs used by activists to target organizations within the industry to anticipate potential future actions.

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

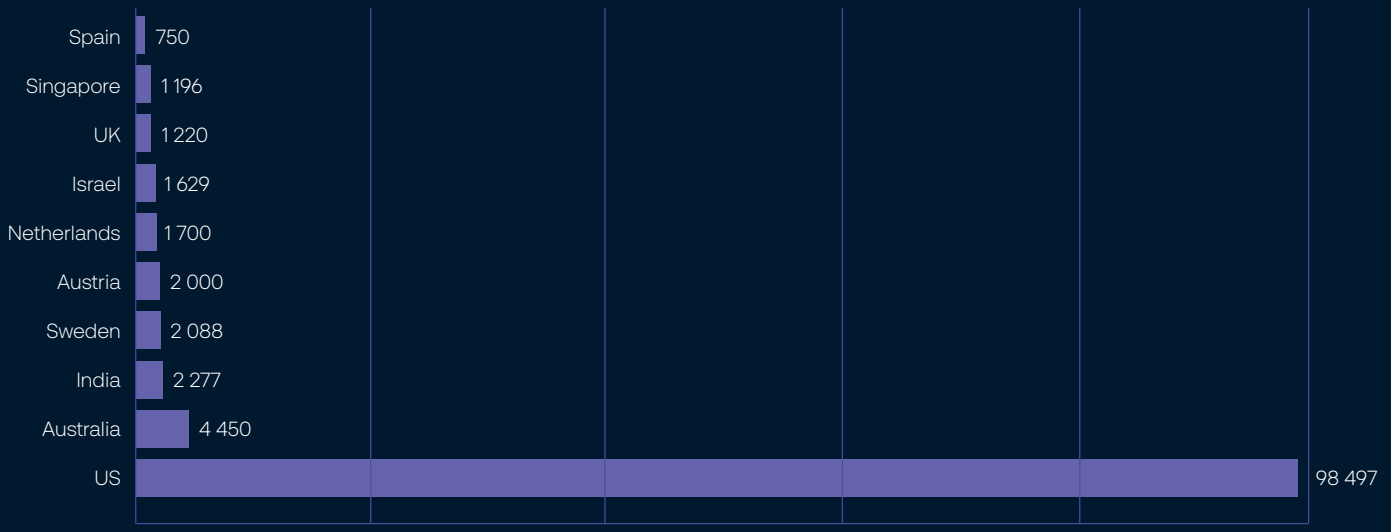
Vast developments in AI continue to be integrated into businesses, leading to roles with primarily AI-capable tasks being made redundant. Large-scale layoffs from AI automation have given rise to backlash from current and former employees, as well as promoting anti-AI / anti-corporate sentiment among residents impacted by AI infrastructure expansion. The Challenger report states that AI is the leading reason for job cuts, which rose to 38% in April, primarily occurring in companies within the technology sector.

However, there are ongoing claims that organizations are using AI to justify redundancies that are in reality attributed to poor performance, over-hiring, market conditions, or cost-cutting, using AI as a scapegoat to prevent backlash and exposing the organization to possible litigation. For example, Sam Altman, CEO of OpenAI, termed this trend as 'AI washing' in a speech at the AI Impact Summit in February, used by executives to avoid looking like "the bad guy." This is evidenced by data that suggests 80% of organizations that reduced their workforce for AI projects did not report better financial results.

- AI-related layoffs are highly likely to continue throughout 2026, considering the high value benefits for organizations regarding streamlining and financial costs. The possibility of further advancements in AI replacing more complicated roles outside of automated tasks, potentially increasing overall competitiveness and volatility in the job market, cannot be ruled out.

- Mass layoffs are likely to create brand / reputational damage as well as disgruntled employees who are likely to utilize organizational restructures as opportunities to form opposition groups and potentially heighten the threat landscape regarding insider risk and corporate espionage. It is also likely to deter prospective employees from applying to organizations experiencing large structural changes due to AI.

Global technology industry layoffs in 2026 (Jan-May)



Significant developments

Date	Location	Description
20 May	Global	Meta announced it will make ~8,000 job cuts to take place from 20 May, reportedly 10% of their global workforce, as part of internal restructuring of operations in favor of AI-first priorities, emphasizing automation and machine-assisted development workflows.
13 May	San Jose, US	Cisco CEO Chuck Robbins announced the company was cutting "fewer than 4,000 jobs" as part of a restructure to increase focus on AI.
7 May	San Francisco, US	Internet infrastructure and cyber security company Cloudflare announced a 20% job cut due to AI adoption.
5 May	San Francisco, US	Coinbase CEO Brian Armstrong announced layoffs affecting ~14% of the workforce, citing AI adoption as a factor.
11 Jan	San Francisco, US	Autodesk, a US software design company, cut its workforce by ~7% to redirect funding towards AI and cloud platforms.

Advisory

- Maintain vigilance of insider threats, particularly with upcoming organization restructures, and review high security clearances that allow access to sensitive data that can potentially be exploited.
- Monitor staff sentiment pre-announcement and ensure all communications remain confidential until proper legal frameworks are in place and ultimate decisions have been made.
- Review organizational and infrastructure resiliency to ensure operational continuity and limit reputational damage to the organization.

Rise in protectionist policies to safeguard sovereign resilience

The rise in protectionist policies has not only persisted into 2026 but has become more entrenched in major economies, incited by escalating geopolitical tensions and conflicts, national security imperatives, and geoeconomic confrontation, a risk framed as the top short-term global risk for 2026 by the World Economic Forum (WEF). This dynamic has largely been driven by increasing geopolitical competition between China and the US and the gradual shift from a US-dominated international order to a multipolar world order. It has sustained elevated market volatility and economic uncertainty for organizations, particularly those reliant on globally integrated supply chains, and has repeatedly impacted third-party countries and organizations. Concurrently, the onshoring of manufacturing and critical services has accelerated, reflecting a longer-term market adaptation that prioritizes resilience and control.

- The use of protectionist policies will almost certainly continue to be a common option for countries and sectors to safeguard sovereign resilience in response to persistent geoeconomic confrontation motivated by differing / incompatible economic systems, political priorities, and strategic goals. This will highly likely increase the use of trade as a tool for political leverage, serving as a self-reinforcing cycle, and incite further adaptation of cross-border security postures.

- The reactive nature of these changes will highly likely force changing market landscapes, altering supply chains, and varying supply-demand. Such variables will likely have a broader impact on international commercial and affiliate relations, requiring the reconsideration of existing / prospective contracts and the reconfiguration of regional strategic and operational needs to limit possible disruption.

Significant developments

Date	Location	Description
2 May	China	China issued a prohibition order declaring that Chinese firms and individuals must not recognize, enforce, or comply with U.S. sanctions targeting five Chinese petrochemical companies for their alleged involvement in Iranian oil transactions.
26 Mar	UK	The UK categorized shipbuilding as a critical national security sector, allowing the government to favor domestic suppliers.
6 Mar	US	The US Cyber Strategy for America mandated that critical infrastructure providers phase out products from adversarial vendors in favor of US-made or allied solutions, targeting Chinese technology.
6 Jan	China	China imposed strict export controls against Japan on critical materials, including gallium, germanium, graphite, and rare earth magnets, to limit the country's defense and high-tech capabilities.

Advisory

- Monitor geopolitical narratives and conflicts in countries housing operations, considering escalations in strategic direction planning for possible shifts in markets and international commercial relations.
- Ensure robust and dynamic security postures along all supply chains, capable of adapting to rapidly changing demands to prevent significant vulnerabilities should changing policies necessitate altered operations.
- Liaise with vendors / third-party suppliers, such as logistic providers, to ensure uniform vetting is applied to all personnel.

Threat actors exploit vulnerable public and private events

The trend of threat actors targeting large-scale events has carried over into 2026, due to the perception that they are the ideal environment to influence decision-making, reach high-value targets (HVT), and raise awareness of their actions. This has been clearly displayed throughout the ongoing event season across Europe, which has seen the consistent targeting of organizations deemed complicit in geopolitical conflicts, such as the Gaza-Israel conflict, and facilitating sociopolitical issues, such as climate degradation, through maintained controversial business practices and contentious commercial affiliations. The tactics, techniques, and procedures (TTPs) used by threat actors have predominantly remained consistent, typically involving activists protesting outside and inside events, blockading venues, and disrupting speeches.

- Threat actors are almost certain to continue targeting organization-specific / industry-wide events, aiming to disrupt proceedings and influence decisions in line with their cause.

The TTPs will likely mirror those previously used, allowing for the implementation of mostly effective security measures, although as campaigns adapt and threat actors show an increasing hybridization, there is a realistic possibility that TTPs will show more frequent signs of escalation.

- While events are typically removed from areas of usual operations and business properties, the targeting of typically high-profile events poses the realistic possibility of causing reputational / brand image damage among both external attendees and employees, likely inspiring motivations for insider threats. This likely has the potential to impact commercial relations, prompting affiliates to withdraw from joint ventures to prevent controversy.

Doxxing

The release of an executive's personal information, which can then be used by threat actors to target the individual both physically or virtually.

Swatting

False emergency calls to disrupt the event and to put the executive in a heightened emotional state.

Deepfakes

Have the potential to be used by threat actors to impersonate an executive, posing a significant threat, especially to virtual events.

Physical assault

Identification of an executive's PII ahead of or during an event has the potential to expose them to physical threats, especially if traveling using public transport.

Cyber attacks

Executives attending events virtually are under increased threat from cyber attacks, potentially using stolen data to disrupt the event / expose private business matters.

Insider threats

Threat actors identify individuals close to the executive to act as an insider threat during the event, to harm the executive or company.

Harassment

Virtual or physical harassment to intimidate the executive, potentially inciting changes to the executive's decision-making during the event.

Trolling

Use of the executive's personal information to impersonate them, potentially to disrupt the event / the individual's reputation.

Significant developments

Date	Location	Description
7 May	London, UK	The Palestine Solidarity Campaign (PSC) disrupted Barclays' event to denounce their alleged investments in defense organizations that arm Israel. Activists stood in the audience chanting and holding the Palestinian flag, while other activists protested outside the venue.
29 Apr	Buenos Aires. Argentina	Extinction Rebellion (XR) Argentina disrupted the panel at the Economic, Finance, and Investment (EFI) Expo to denounce the attendance of mining organizations.
26 Mar	Stockholm, Sweden	Greenpeace Sweden blockaded the event of Essity to denounce their affiliation with Svenska Cellulosa Aktiebolaget (SCA), which allegedly conducts environmentally damaging business practices.
4 Feb	London, UK	Fossil Free London (FFL) disrupted Equinor's quarterly results meeting due to the company's alleged complicity in the Gaza-Israel conflict.
29 Jan	Trondheim, Norway	Students for Palestine Trondheim, Spire, and Scientist Rebellion protested next to the stands of organizations deemed complicit in the Gaza-Israel conflict at networking events held by the Norwegian University of Science and Technology (NTNU).

Advisory

- Operate high levels of operational security (OPSEC) before and during the event, keeping open-source information about the event to a minimum. This includes the location of the event, the scheduled timings, and expected attendees.
- Conduct appropriate due diligence on attendees to reduce the possibility of threat actors legitimately entering the event.

Sustainability concerns disrupt resource-intensive infrastructure projects

In line with political priorities, globalization, and market demand, 2026 has continued to see the planning, construction, and operation of resource-intensive infrastructure projects despite sustainability concerns, although there have been instances suggesting key players are transitioning to a more impact-conscious approach. Previously, decisions shaped by strategic and economic goals have seen the legal, regulatory, and fiscal boundaries eased for such infrastructure, including the subsidization of data center projects. While these priorities remain, the UK and the US have introduced laws aiming to alleviate the burden of resource-intensive infrastructure projects on public infrastructure and prevent the general public from facing increased costs, seemingly heeding to sustainability concerns and persistent criticism / protest movements.

- While legal and regulatory changes concerning resource-intensive infrastructure suggest a political receptivity towards sustainability, there is limited evidence to suggest that this marks a total transition that will address all sustainability concerns, with further measures highly likely to be shaped by political agendas and international markets. Public efforts against resource-intensive infrastructure projects will almost certainly continue in the immediate term.
- Organizations will almost certainly continue to face significant backlash from individuals and groups holding sustainability concerns, likely transpiring into online campaigns that have the potential of materializing into physical mobilizations that pose risks to operational and site security. Fluctuating political direction will likely complicate the establishment of realistic strategic planning.

Significant developments

Date	Location	Description
1 May	Memphis, US	Environmental activists blockaded the entrance to xAI's data center to protest the facility's gas-powered turbines.
4 Mar	Washington DC, US	US President Donald Trump passed the Ratepayer Protection Pledge to ensure high energy demands from AI data centers do not cause an increase in the electricity bills of neighboring households.
27 Feb	London, UK	Parliament launched an investigation into the energy use, water consumption, and climate impacts of data centers, explicitly citing public concern.
10 Jan	Dorr Township, US	A small group of protestors, predominantly residents of Dorr Township, protested near the site of a proposed Microsoft data center, citing concerns over water consumption, electricity consumption, and pollution.

Advisory

- Schedule community consultation and engagement in areas of interest to assess public sentiment towards the construction of resource-intensive infrastructure in the area and identify possible points of contention that could lead to backlash.
- Maintain awareness of online sentiment surrounding resource-intensive infrastructure specific to customer needs and direction to understand controversies.
- Monitor changes to local and regional regulations that could cause changes to the construction and operation of resource-intensive infrastructure.

Authorities' response to drone threat encourages further exploitation

The continued use of drone technology by threat actors over sensitive locations remains a prominent threat to organizations globally, continuing to enable hostile reconnaissance and providing opportunities to disrupt operations. While certain national governments and other relevant authorities have taken steps to mitigate the risk posed by unauthorized drones, the scale and nature of the challenge mean this is unlikely to prevent exploitation in the short-to-medium term. Increasing levels of state-backed espionage tactics remain a primary threat to Western critical national infrastructure (CNI) as well as large-scale events hosting high-profile individuals, particularly as China and the US compete to achieve technological superiority during a period of increased geopolitical competition. The commercial availability of unmanned aerial systems (UAS) allows threat actors to conduct low-level sabotage and disruptive actions that have the capacity to pose low to moderate operational disruptions to organizations.

As China's Da Jiang Innovations Science and Technology Company (DJI) dominated the global drone market in 2024, DJI drones are heavily involved in a variety of Western industries, heightening the threat landscape posed by state-backed actors. Despite this, the US Commerce Department withdrew recent planned restrictions on imports of Chinese made drones, claiming that the proposed measures would cause undue harm to US stakeholders. However, the Federal Communications Commission's (FCC's) ban on new drone models remains in place.

- Security concerns from state-sponsored drone activity will almost certainly persist in 2026, particularly with hesitancy from the US administration to further ban China-manufactured drones. However, alternative measures to counter growing threats, such as anti-drone technology, will be highly likely be implemented at large-scale events, particularly those hosting high-profile individuals.

- Organizations operating in the CNI sectors, aerospace and defense, or other industries deemed critical for national security are likely to be targeted by adversaries using drones due to the continued commercial availability of such devices, potentially facing low-moderate operational disruptions. Businesses are likely to experience reduced operational capacity, impacting customer confidence and leading to financial losses in the short term.

Significant developments

Date	Location	Description
23 Apr	Washington DC, US	US Republican Senator for Arkansas, Tom Cotton, introduced legislation aimed at increasing the legal authority of private sector companies to protect domestic CNI sites from drones.
13 Jan	New York, US	The US is seeking to invest $115 million in counter-drone technology to increase protection at FIFA World Cup venues amid America's 250th Anniversary celebrations.
11 Jan	Stockholm, Sweden	The Swedish government announced plans to invest $1.6 billion in air defenses aimed at protecting civilians and critical infrastructure.

Advisory

- Monitor legislative changes to counter drone capacity and leverage legal rights to implement appropriate measures from drone threats to sensitive sites.
- Remain vigilant of aerial reconnaissance vulnerabilities, ensuring necessary incident response plans (IRPs) are in place.
- Maintain awareness of banned drone models and report to authorities of suspicious behavior.

Risks to organizations from increased dependency on cloud environments

The operational shift toward cloud-based Software-as-a-Service (SaaS) has continued into 2026, bringing with it larger attack surfaces and vulnerabilities inherent to new identities, integrations, and configurations, such as outages, breaches, and misconfigurations. The development of cyber attack capabilities has enhanced vulnerabilities, creating a faster and more adaptive threat landscape, and AI continues to serve as a threat multiplier, enabling compressed attack lifecycles and automated reconnaissance. However, threat exposure has evolved beyond purely digital targeting, with 2026 highlighting the physical and geopolitical risks posed to cloud providers, which are directly inherited by dependent organizations through operational disruptions and digital infrastructure disturbances.

- Cyber-based risks associated with cloud-based SaaS are almost certain to evolve in the immediate term, adapting to evade security measures, and further complicating the threat landscape for both vendors and cloud-dependent organizations. Physical threats are highly likely to correlate with geopolitical escalation and kinetic warfare, with data centers and cloud infrastructure almost certain to continue being identified as vulnerable targets that support / enhance military capabilities.

- Risks posed by increased dependency on cloud environments will almost certainly continue to incite financial incursions, operational disturbances, and digital disruptions that are increasingly difficult to guard against. While this is unlikely to see a complete reversal of cloud adoption, further security incidents are likely to necessitate operational and security cooperation between vendors and users, potentially seeing the intervention of regional / state regulations to prevent large-scale disruption and address national security concerns.

Significant developments

Date	Location	Description
11 Mar	Tehran, Iran	The Iranian Islamic Revolutionary Guard Corps (IRGC)-affiliated Tasnim News Agency announced that data centers and digital infrastructure across the Middle East were *"legitimate targets"* during the Iran conflict.
1 Mar	Bahrain	Two Amazon Web Services (AWS) data centers were hit by Iranian drones during the Iran conflict, causing multi region service degradation, application downtime, and data access failures.
2 Feb	Global	An outage in Microsoft Azure, triggered by a misconfiguration, caused a 10-hour outage that impacted several services across multiple regions, particularly in the US.
Jan	Global	Cyber threat group ShinyHunters coordinated a global phishing / vishing campaign, gaining access to Microsoft Entra and breaching organizations within the SaaS.

Advisory

- Maintain local, offline access for essential / vulnerable operations, such as payroll and customer data, through critical-path mapping that allows the implementation of effective incident response plans (IRPs) should cloud services be compromised.
- Strengthen identity and access controls across all digital infrastructure and ensure efficient and immediate detection programs are active.
- Enhance network security through software-defined microsegmentation to isolate sensitive and vulnerable internal systems, preventing the spread of breaches between departments and systems.

Information landscape threatened by emerging GenAI

The rapid advancement in AI and decline in institutional trust have only accelerated in 2026, further worsening the credibility of the information landscape through hyper realistic synthetic content, including text, images, audio, and videos, that outpace society's ability to authenticate them. This combination has made corporations vulnerable to market manipulation, operational disruption, financial loss, and AI-driven reputational risks, to which an estimated 58% of organizations have been exposed. The risks of GenAI, including misinformation and distrust, are deemed prominent global threats by the World Economic Forum (WEF). However, there has been a 190% increase in AI-detection platforms over the last two years, indicating a potential shift towards addressing the 'AI panic'.

The material impact of GenAI has been seen across political spheres, where lines have been blurred between authentic and fabricated political communication, making it harder for voters to verify online material. This continues to raise concerns about misinformation, voter manipulation, and an erosion of institutional trust, notably while a patchwork of state rules and voluntary industry standards struggles to address vulnerabilities exposed by GenAI.

- The information landscape will almost certainly continue to be threatened by emerging GenAI capabilities throughout the long term, notably as the development and evolution of AI remains a market demand and a strategic priority for organizations. Threat actors likely deem GenAI as a non-resource-intensive, cheap, and accessible method to target organizations with which they have grievances, likely motivated by geopolitical or socio-political ideologies.
- Impacts of sustained information disorder through GenAI will likely predominantly remain reputational, impacting public perceptions of business practices, market credibility, and C-suite executives. However, in severe cases, the uncertainty surrounding the legitimacy of GenAI could see a decline in customer bases and a degradation in commercial relations, or be used to defraud organizations.

Significant developments

Date	Location	Description
20 Mar	Online	Pro-Iranian accounts published AI-generated footage claiming to show an intercepted US F-35 fighter jet.
26 Feb	Rome, Italy	The Bank of Italy issued a warning of potential scams involving fake articles, images, and videos in which Governor Fabio Panetta endorses investment products.

Advisory

- Enhance monitoring for disinformation about the organization through social-listening tools to detect incidents in real time.
- Create an incident escalation protocol that allows the efficient reporting and effective handling of GenAI risks to the organization.
- Maintain verified channels, such as social media platforms and newsletters, that can be used to counter disinformation campaigns.

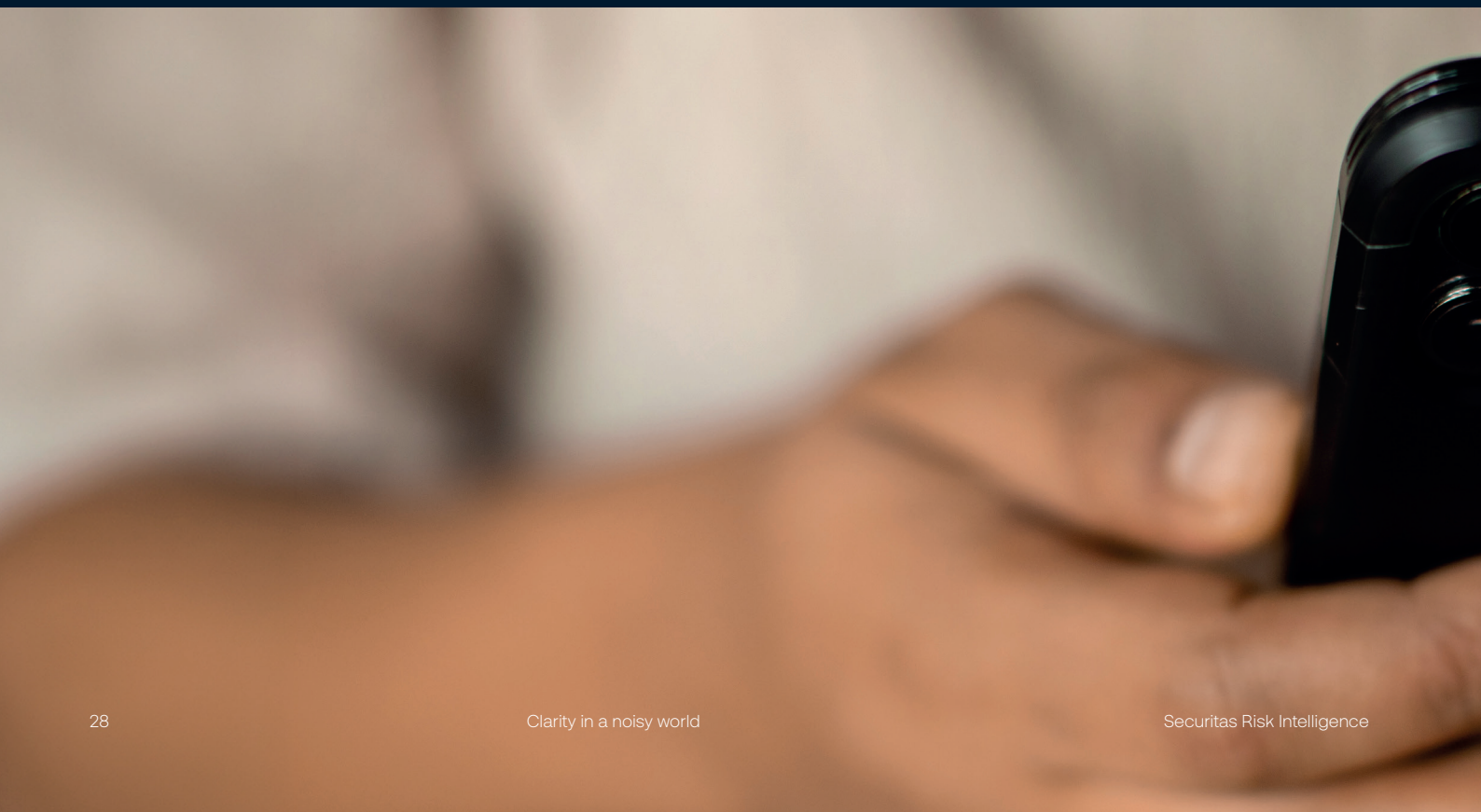
Social media platforms increasingly exploited to orchestrate high-impact doxxing campaigns

Threat actors have continued to utilize social media to circulate personally identifiable information (PII) in information disorder campaigns (mis / dis / malinformation) throughout 2026. Obtaining and spreading PIIs remains a sought-after tactic to pressure organizations and ascertain control over policy decisions. Disinformation ecosystems weaponize leaked or fabricated personal data to intimidate individuals and polarize communities, contributing to a erosion of trust and social cohesion.

The widespread availability of AI-powered data-scraping technologies has made it easier for malicious actors to harvest and expose personal information, transforming doxxing from harassment into organized digital persecution targeting journalists, public officials, educators, and healthcare workers.

State-sponsored hacktivists driven by geopolitical tensions, following the outbreak of the Iran conflict on 28 February, are likely to conduct doxxing campaigns targeting corporate employees from adversary states perceived to be state-linked.

- Threat actors are highly likely to maintain sustained pressure through social media doxxing campaigns against target organizations, particularly as security measures against physical threats become more readily available, reducing the possibility of in-person actions. Increasing online doxxing campaigns have the realistic possibility of influencing restrictive policies on social media use and possibly restricting employee access to sensitive company data to prevent leaks.
- Further advancements in AI are highly likely to be leveraged by threat actors to circulate information disorder surrounding the company and C-suite executives, potentially triggering the implementation of additional security measures, which are likely to incur additional costs for the organization. The possibility of heightened cyber threats from the exploitation of employee PIIs and ransomware cannot be entirely ruled out.

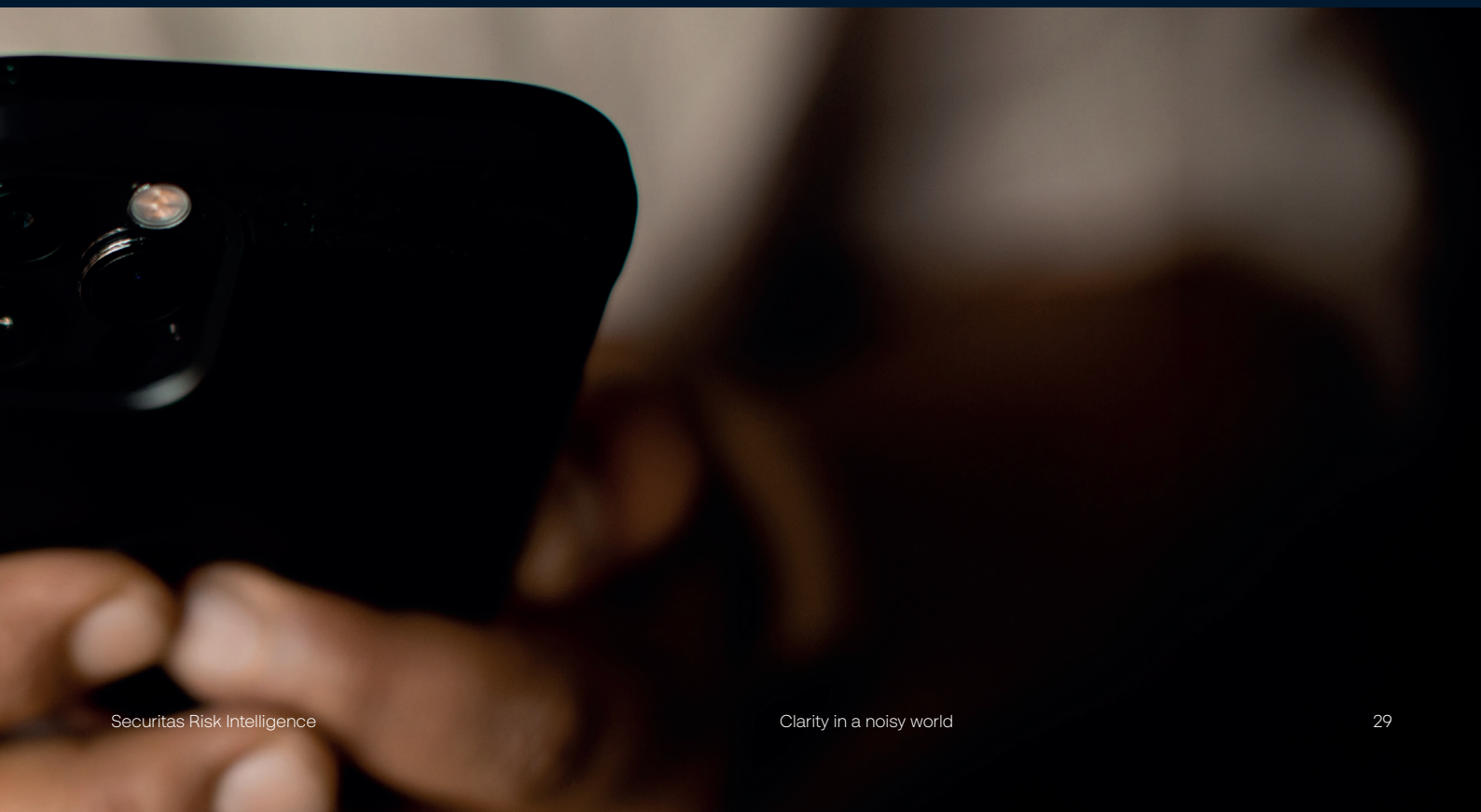


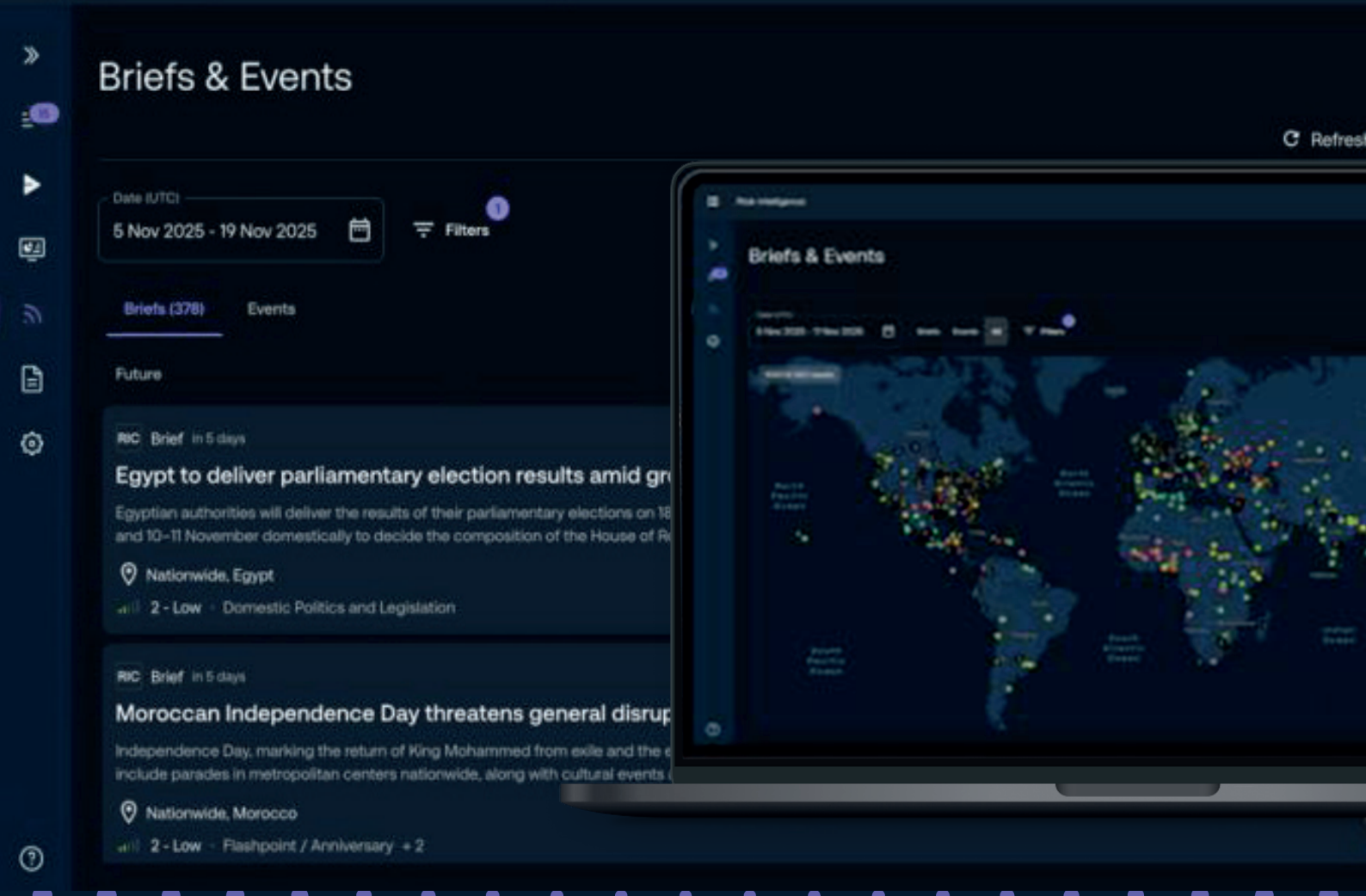
Significant developments

Date	Location	Description
11 May	Exton, US	West Pharmaceutical Services disclosed that it experienced a cyber attack that led to data loss and the encryption of some systems, disrupting global operations.
29 Apr	US	Iran-linked hacker group, Handala, reportedly leaked the personal data of more than ~2,000 US Marines, including home addresses, and issued direct threats claiming individuals are under surveillance.
22 Jan	France	A cyber threat actor named 'Idopanda2' leaked sensitive files belonging to France-based aerospace firms.

Advisory

- Consistent monitoring of open source platforms is advised, especially following major policy changes to the organizations that are likely to be considered controversial.
- Implement an appropriate incident response plan (IRP) to ensure dis / misinformation online regarding the organization gains limited media attention and that necessary statements are issued to minimize reputational harm.
- Conduct appropriate reviews of online doxxing campaigns to assess the level of threat and intent and inform employees of online safety procedures.




Briefs & Events
Refres
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 gr
Egyptian authorities will deliver the results of their parliamentary elections on 18
and 10–11 November domestically to decide the composition of the House of R
Nationwide, Egypt
2 - Low · Domestic Politics and Legislation
RIC Brief in 5 days
Moroccan Independence Day threatens general disrup
Independence Day, marking the return of King Mohammed from exile and the e
include parades in metropolitan centers nationwide, along with cultural events
Nationwide, Morocco
2 - Low · Flashpoint / Anniversary + 2
Briefs & Events

Global

2

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

A series of large-scale anti-government protests primarily conducted by youth populations under the ‘Gen Z’ banner played a prominent role in shaping the global protest landscape throughout 2025, with such movements forcing regime change in Madagascar and Nepal and causing significant unrest in countries including Algeria, Mexico, Morocco, and Peru. While youth-led protests took place in Uganda following the country’s general election in January 2026, protest activity ascribed to the ‘Gen Z’ movement has been limited throughout the first half of 2026.

Previous ‘Gen Z’ protests have been driven by high rates of youth employment, poor economic opportunities, social inequality, corruption, and other specific socio-political issues. The movement has been widely characterized by activists using Discord, Signal, Telegram, and other traditional digital platforms to organize / communicate, and the use of popular symbols such as a pirate flag from the animated series One Piece.

- Although ‘Gen Z’ protest activity has been limited, the social, political, and economic factors that drove such movements in recent years continue to be present in many countries across the Global South, meaning that further demonstrations remain probable in the short to medium term. Fuel shortages caused by the ongoing Iran conflict (specifically the continued closure of the Strait of Hormuz) are highly likely to exacerbate the risk of protests, particularly in parts of Southeast Asia that heavily rely on fuel imports from the Middle East.
- Countries that experienced significant unrest during previous ‘Gen Z’ protests, or are concerned about the potential for similar unrest, are highly likely to implement new measures to increase control of the digital information landscape to disrupt the ability of youth groups to communicate, coordinate, and organize in digital spaces. Potential measures include routing all international traffic through a single, state-controlled choke point that allows deep packet inspection (DPI), enabling authorities to block specific keywords or encrypted protocols without a full shutdown, implementing new data localization laws, pressuring social media platforms to alter discovery algorithms, or artificially throttling certain platforms.

Significant developments

Date	Location	Description
16 Jan	Kampala, Uganda	At least seven people were killed, and three were injured in clashes between police and political opposition supporters following the country’s presidential election.

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 plans 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.

US economic policy sustains global uncertainty and risk

US economic policy has continued to serve as a significant driver of economic uncertainty and risk over the last six months. US President Donald Trump's administration continues to leverage the country's significant global economic influence to pursue its strategic objectives, using tariffs (or the threat of tariffs) to pressure other countries into changing policies or making concessions in negotiations with the US. Economic policy changes have been announced with little to no notice, often first being referenced in a post on Trump's Truth Social platform.

Domestic legal challenges have further exacerbated global economic uncertainty. Trump initially utilized the International Emergency Economic Powers Act (IEEPA) to implement global 'reciprocal' tariffs; however, in February, the Supreme Court ruled this legislation does not give the president unlimited authority to impose import taxes under the guise of an "emergency," allowing the US Court of International Trade to later instruct the government to begin refunding all importers of record who paid IEEPA-based duties. The administration is now utilizing Section 122 of the Trade Act of 1974; however, this was also found to be unlawful in an ongoing legal case on 7 May.

- The Trump administration will almost certainly continue using the US's significant economic influence to shape the behavior of other countries. This is highly likely to be unpopular across the international community and strain diplomatic relations, including with countries historically aligned with the US, and encourage further economic diversification efforts among prominent US trade partners.

- Uncertainty surrounding US economic policy and the legality of existing tariffs will almost certainly encourage businesses to delay capital expenditures due to the current difficulty of calculating landed costs and return on investment figures. Economic volatility is likely to have the largest impacts on smaller businesses that are less equipped to over-order / pre-ship a large number of goods ahead of tariff deadlines or absorb price fluctuations.

Significant developments

Date	Location	Description
8 Apr	US	Trump announced the imposition of 50% tariffs on any country supplying military weapons to Iran.
26 Mar	Germany	Reports emerged that German officials had begun preparing a comprehensive plan to identify vulnerabilities in US supply chains to inform German and EU means for applying pressure on the US amid strained EU-US relations, partly driven by US economic policy.
4 Mar	US	A judge at the US Court of International Trade directed the Trump administration to begin the process of refunding over $130 billion in revenue generated by the administration's former 10% baseline tariff.
20 Feb	Global	Trump announced a new 10% global tariff after the Supreme Court ruled against the Trump administration's global 'reciprocal' tariffs.
29 Jan	Cuba	Trump imposed a tariff system on imports into the US from any country that directly or indirectly sells / provides oil to Cuba as part of broader efforts to destabilize the island's government.
17 Jan	EU	EU lawmakers signaled they would not approve the EU-US trade deal after Trump threatened to impose new tariffs on eight European countries as part of efforts to gain control of Greenland from Denmark.

Advisory

- Consider developing escalation plans to guide decision-making amid rapidly shifting regulations, with consideration for operational continuity in affected regions.
- 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).

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

The threat posed by the increasing presence of extremist content, terrorist manifestos, and ideological propaganda on mainstream social media, gaming platforms, and decentralized file-sharing sites has increased significantly over the last six months due to the Iran conflict's influence on the global terror threat landscape.

In the days following the death of Iranian Supreme Leader Ali Khamenei, Al-Qaeda's Cyber Jihad Movement (CJM) issued a statement announcing its official entry into the conflict and calling upon *"believing men and women"* to join *"Global Cyber Jihad"* and inflict *"financial loss and cyber disruptions"* on the Arab, Indian, Israeli, Pakistani, and US governments. This was followed by the Islamic Revolutionary Guard Corps (IRGC) affiliated Tasmin News amplifying Ayatollah Nouri Hamedani's fatwa, declaring it *"obligatory upon every Muslim, anywhere in the world, to avenge the blood of martyr Imam Khamenei"* and that *"anyone killed this way will be considered a martyr."* These calls to action have been accompanied by Iranian / aligned groups disseminating significantly increased amounts of propaganda intended to radicalize sympathetic groups and encourage self-radicalized individuals to take action.

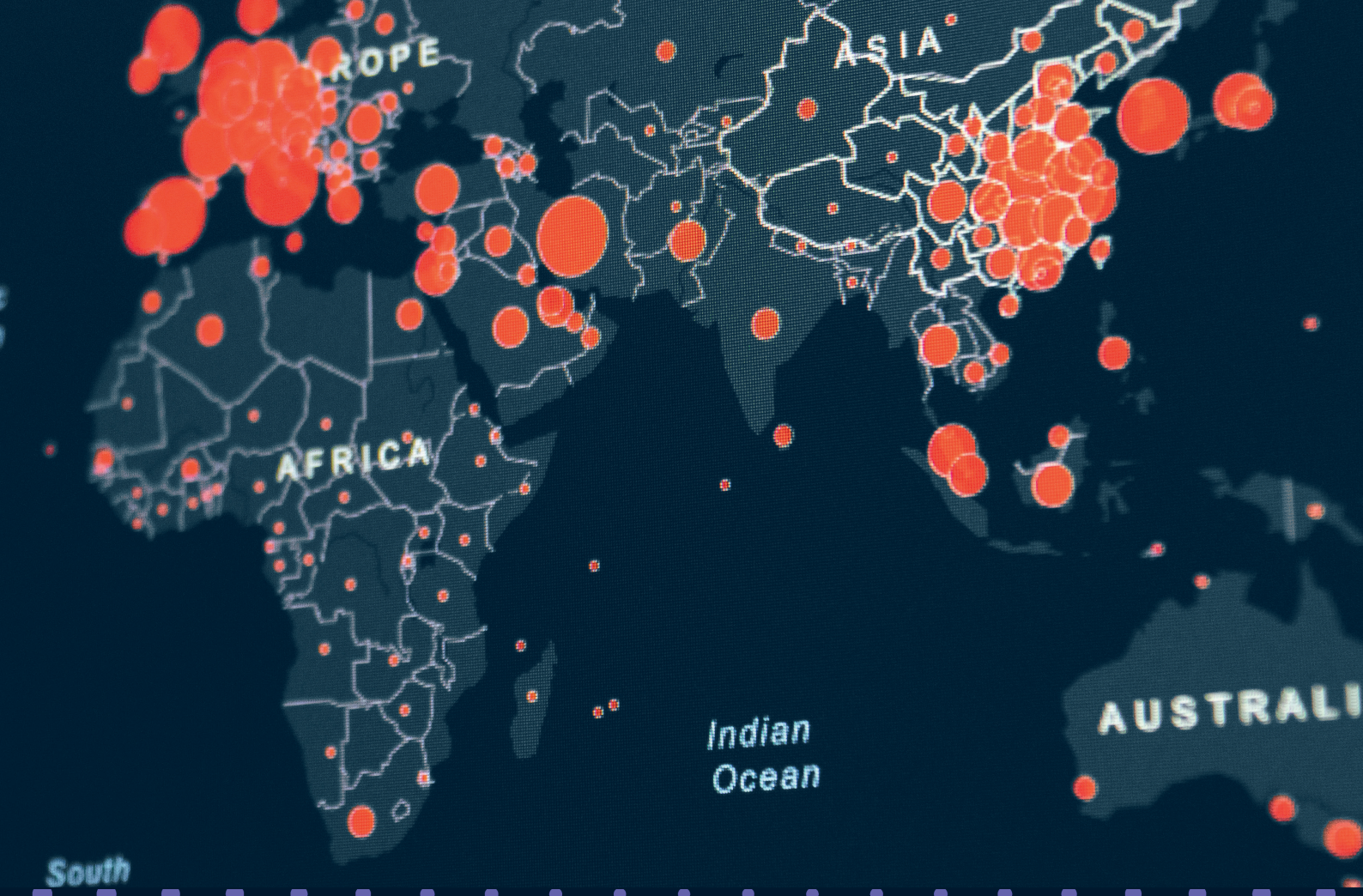
- The proliferation of terror materials on open-source platforms almost certainly represents a long-term threat to the global security landscape. State and non-state actors utilizing gray-zone warfare (GZW) are highly likely to continue disseminating terrorist materials to encourage radicalized supporters to carry out self-initiated attacks. This threat is likely to be exacerbated by the increasing availability of drones, 3D printers, and other technology allowing individuals to conduct sophisticated attacks.
- Web-hosting services and online platforms are highly likely to face increasing scrutiny from regulators as authorities attempt to combat the prevalence of radicalizing extremist content and ideological propaganda in digital spaces. This is likely to necessitate potentially disruptive and costly operational changes and introduce new compliance-related challenges.

Significant developments

Date	Location	Description
7 May	Global	Al-Qaeda in the Arab Peninsular (AQAP) recirculated a pipe bomb construction manual and called on its followers to repeat the Bondi Beach terror attack in Europe and the US.
23 Mar	Antwerp / Brussels, Belgium	Belgium deployed military personnel to protect Jewish communities in Antwerp and Brussels after a series of terror incidents claimed by Iran-aligned Harakat Ashab al-Yamin al-Islamiyya (HAYI) in Belgium and elsewhere across Europe.
12 Mar	West Bloomfield, US	A naturalized US citizen born in Lebanon drove an explosive-laden vehicle into a Jewish Reform synagogue before being fatally shot by security personnel after being inspired by Hezbollah.
11 Feb	Podkarpackie, Poland	Polish authorities charged an 18-year-old man with plotting to attack a school in the southeastern Podkarpackie region and inciting violence and hatred on religious grounds via the internet.

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.



AMEA

3

Middle East security landscape complexifies following Gaza ceasefire

The Middle East continued to be the global epicenter of geopolitical risk and uncertainty throughout the first half of 2026 due to major developments across the Persian Gulf significantly intensifying pre-existing regional instability that has gradually been increasing since the Iran-Israel 'shadow war' evolved into an outright confrontation with the escalation of the Gaza-Israel conflict in October 2023. The US began joint strikes with Israel against targets across Iran as part of 'Operation Epic Fury' on 28 February, shortly after Iran experienced a wave of mass anti-government protests that were violently repressed by government forces. Iran responded by closing the strategically important Strait of Hormuz and launching drone / missile strikes on Israeli-US targets across the region, and critical national infrastructure (CNI) viewed as facilitating US military operations. Regional Iranian proxies also increased activity.

The operation's stated aim was to overthrow the Iranian government and destroy the elements of the Iranian nuclear program that survived 'Operation Midnight Hammer' in June 2025. At the time of reporting, neither of these goals has been verifiably achieved, and a fragile ceasefire has remained in place since 8 April to facilitate negotiations. Diplomatic efforts have stalled over disagreements related to the Strait of Hormuz and Iran's nuclear program.

- Despite the ongoing ceasefire and diplomatic engagement, the risk of escalation, including renewed Israeli / US strikes on Iran and Iranian strikes in the Gulf, remains high, particularly while negotiations remain stalled. Iran and the US are likely to continue prioritizing maritime pressure in the Strait of Hormuz, sustaining disruption to shipping flows and maintaining upward pressure on global energy prices. Iran and the US will likely continue to engage in either direct or indirect negotiations in the immediate to short term; however, persistent disputes over Iran's nuclear program and the Strait of Hormuz, together with volatile rhetoric and sporadic kinetic military activity, will almost certainly continue to hinder progress towards a permanent settlement.

- The Iran conflict has intensified the global threat landscape, presenting a range of challenges for organizations globally. Ongoing tensions will highly likely motivate further protest actions across multiple countries, including mass protests in major cities and isolated direct targeting of organizations linked to Israel / the US, while also increasing the risk of terrorism across Israel and the West. Restrictions on movement will almost certainly disrupt transport / logistics, particularly if implemented with little warning.

Significant developments

Date	Location	Description
8 Apr	Gulf Region	A ceasefire between Iran and Israel / the US came into force to allow negotiations for a peaceful resolution to the conflict.
16 Mar	Southern Lebanon	The Israel Defense Forces (IDF) began ground operations in southern Lebanon in response to Hezbollah resuming rocket strikes on Israel after the outbreak of the Iran conflict.
28 Feb	Gulf Region	Iran began attacks on targets across the Gulf and effectively closed the Strait of Hormuz in response to joint Israeli-US strikes, disrupting ~20% of the global oil supply.
28 Feb	Nationwide, Iran	Israeli and US forces attacked targets across Iran as part of 'Operation Epic Fury,' killing Iranian Supreme Leader Ali Khamenei.

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.

MySecuritas Briefs & Events maps showing incidents reported in the first seven days of the Iran conflict escalation on 28 February.

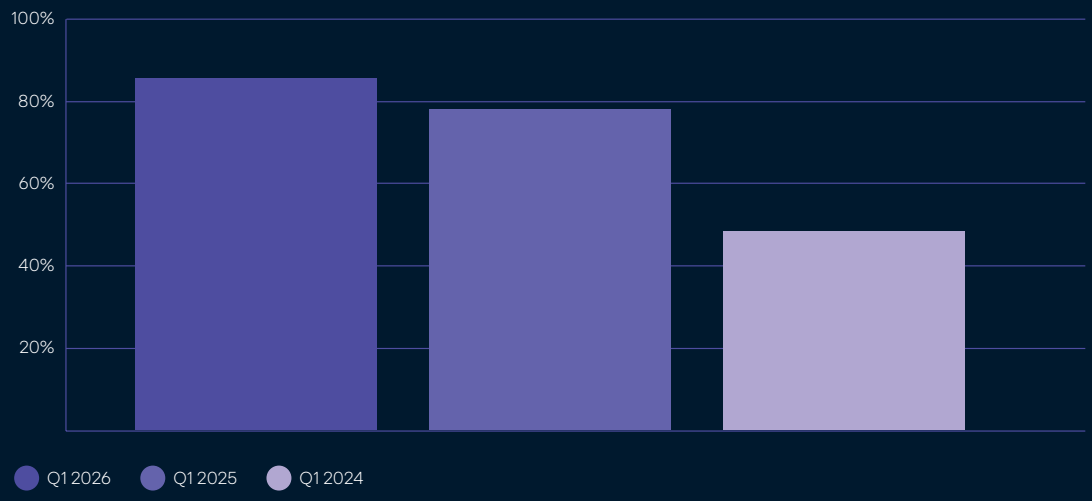
Islamist militants expand activity in West Africa

West Africa's regional security environment has continued to be degraded by actions taken by various Islamist groups, including Boko Haram, Jama'at Nusrat al-Islam wal-Muslimin (JNIM), and the Islamic State (IS) West Africa Province, throughout the first half of 2026, impacting civilians, military infrastructure, government institutions, and business assets, while also influencing the regional geopolitical environment.

The region has become significantly more volatile since the creation of the Alliance of Sahel States (AES), comprised of Burkina Faso, Mali, and Niger, their withdrawal from the Economic Community of West African States (ECOWAS), and the subsequent reduced levels of cooperation on security matters. While AES states experience a significant amount of Islamist-driven violence, insecurity created by these groups extends into neighboring countries, including Benin, Chad, and Niger.

- West Africa's security environment will almost certainly remain volatile while the AES states refuse to engage with neighboring countries and other Western / Western-led peacekeeping missions and rely on the use of Russian mercenary groups to combat Islamist insurgencies. This is highly unlikely while the current governments remain in power due to their anti-Western / anti-imperialist ideologies.
- Persistent militant attacks are likely to exacerbate existing security risks for commercial operations, particularly in transport, logistics, and extractive sectors. Businesses are likely to face sustained increases in security costs, operational delays, and heightened risk to personnel, with a realistic possibility of further disruption if violence escalates. Continued instability is also almost certain to continue undermining investor confidence and constraining economic activity and development.

Data showing the increase in Islamic State (IS) activity in Africa over the last 3 years



Significant developments

Date	Location	Description
25 Apr	Mali	The Malian army reported militants launched a series of coordinated attacks across the country.
22 Apr	Northeastern Nigeria	Suspected Boko Haram militants attacked two villages in Adamawa and Borno states, killing at least 20 people.
22 Mar	Mali	Authorities released more than 100 suspected Islamist militants as part of an informal agreement to halt months of attacks on fuel convoys heading to the capital, Bamako, carried out by JNIM.
6 Mar	Kofouno, Benin	JNIM claimed responsibility for an attack on a military base in Kofouno, northern Benin, which killed at least 15 soldiers.
16 Feb	Nigeria	~100 US military advisors were deployed to provide training, technical support, and intelligence-sharing to government forces to assist in combating Islamist militants.
26 Jan	N.E. Borno state, Nigeria	Suspected Boko Haram militants killed seven Nigerian soldiers and captured 13 others, including their commanding officer.
11 Jan	Western Mali	Hundreds of militants reportedly linked to JNIM attacked multiple industrial sites in western Mali, facilities along National Route 22.

Advisory

- Continuously monitor changes in the security and threat landscape, keeping local employees, suppliers, and key supply chain partners informed of developments, expectations, and requirements.
- Implement and maintain robust security protocols for sites and personnel operating in areas with known militant activity.
- Ensure sites and staff are aware of terrorism-related threats, including kidnappings, and develop, implement, and regularly test response plans for such incidents.

Reemerging markets present opportunities and risks to businesses

Private organizations have continued to invest in emerging / reemerging markets throughout the first half of 2026. Syria has experienced the most significant investment as the country continues to reintegrate itself into the international community and global economy under the leadership of President Ahmed al-Sharaa, marked by the further removal of international sanctions and the normalization of diplomatic / trade relations. This trend has continued despite several instances of violent clashes between government forces and minority groups in several parts of the country and the deterioration of the regional security environment.

Investment has continued in Armenia / Azerbaijan as part of the Trump Route for International Peace and Prosperity (TRIPP) agreed to in August 2025, while the Democratic Republic of the Congo (DRC) is being viewed by some international investors as a *"solution country"* due to its large deposits of rare earths and other critical minerals and Myanmar has reported increased investment into nationally important sectors despite its political landscape remaining volatile.

- 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. However, while progress has been made across several markets throughout 2026, this process is highly likely to extend into the medium to long term, due to the complexities of negotiating and implementing investment deals.

- Despite conflicts de-escalating, the security situation remains fragile in many cases, and investor risk appetite has likely been dampened by global economic uncertainty and financial losses caused by the Iran conflict. 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.

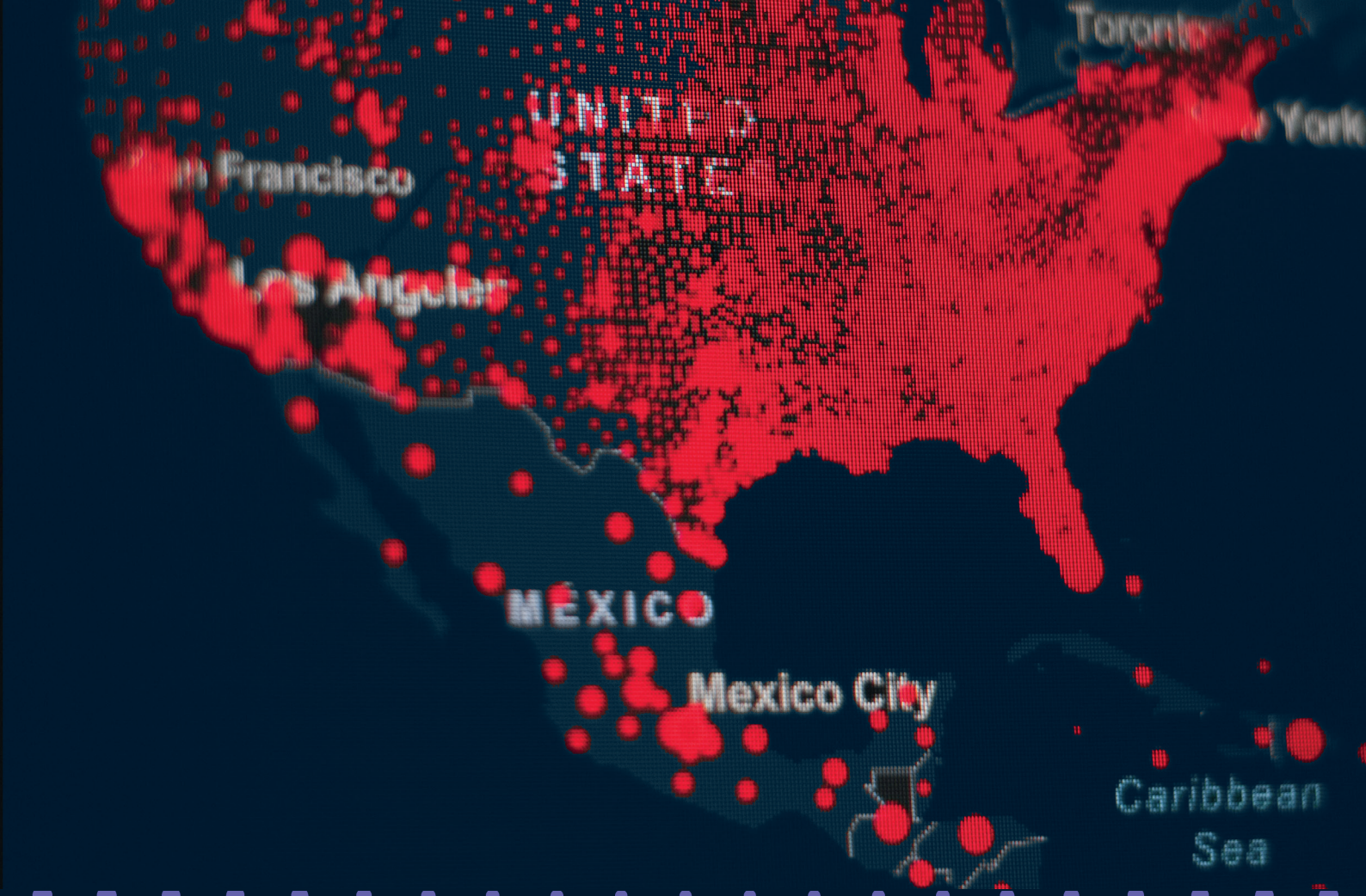
Significant developments

Date	Location	Description
5 May	Kabul, Afghanistan	Authorities announced the Inter-Ministerial Investment Committee had approved 48 investment proposals submitted by domestic and international investors, with initiatives spanning key strategic sectors, including energy and electricity, infrastructure development, construction, agriculture, transportation, and information technology.
1 Apr	Caribbean Sea	International media reported Shell was in advanced talks with Venezuela's government to develop four large areas near Trinidad and Tobago.
20 Mar	Damascus, Syria	President Ahmed al-Sharaa announced the 2026 budget was ~$10.5 billion following significant funding from international investors.

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 / 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.


STANDARD



Americas

4

US reorientation to Latin America exacerbates political uncertainty and regional instability

The US has sustained efforts to increase its political, military, and economic influence over Latin America (LATAM) and the Caribbean region in 2026, as the administration continues to enact the 'Trump Corollary' to the Monroe Doctrine. This was formally outlined in the November 2025 National Security Strategy and aims to ensure the Western Hemisphere remains *"reasonably stable"* and well-governed enough to prevent and discourage mass migration to the US; regional governments cooperate with the US against narco-terrorists, cartels, and other transnational criminal organizations; limit the regional influence of states the US considers adversarial, and ensure continued US access to key strategic locations.

While the Iran conflict has forced the US to focus military deployments on the Middle East, military action and developments have continued even after Operation Absolute Resolve saw the overthrow of Venezuelan President Nicolás Maduro. US Southern Command regularly conducts operations to disrupt illicit maritime activity within the Western Hemisphere and has deployed special operations forces to assist the Ecuadorean and Peruvian governments, while the US has reopened or invested in several military bases across the region. Military operations have been supported by diplomatic efforts undertaken as part of the Shield of the Americas security program, which intends to coordinate military, law enforcement, and intelligence efforts among participating nations.

- The recommissioning / modernizing of US military facilities across the region and increasing cooperation with countries participating in the Shield of the Americas and other regional partners almost certainly has the potential to facilitate long-term deployments of sophisticated military assets. However, it is probable that the US administration will continue to place a greater priority on its interests in the Middle East while the Iran conflict is ongoing, as this is likely considered to pose a larger threat to the US's global security / influence.
- Due to ongoing geopolitical competition with China, and China's significant trade relationship with many of the countries in the region, there is a realistic possibility that the US's renewed interest will force organizations in the region to reevaluate their supply chain and business relationships to be eligible for US investment programs / contracts. It is probable that the US will invest in strategic infrastructure and mining as part of efforts to decouple from Chinese supply chains and protect its economy from geoeconomic volatility.

Significant developments

Date	Location	Description
26 Mar	Buenos Aires, Argentina	Argentina designated the Mexico-based Jalisco New Generation Cartel (CJNG) as a terrorist organization, aligning with US policy.
7 Mar	Miami, US	The US formed the Shield of America with ~17 LATAM states.
20 Feb	Santiago, Chile	The US imposed visa restrictions on three Chilean government officials over allegations that they undermined regional security.
29 Jan	Havana, Cuba	Trump issued an Executive Order declaring a national emergency that imposed a tariff system on imports into the US from any country that directly or indirectly sells / provides oil to Cuba.

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.

Political extremism growing in scope and frequency in the US

Political divisions in the US have persistently widened throughout the first half of 2026, leading to further high-profile manifestations of political extremism. Increasing division has largely stemmed from actions undertaken by US President Donald Trump's administration concerning domestic socio-political issues and foreign policy, alongside domestic opposition to this agenda, and broader geopolitical developments, most notably in the Middle East. Protest and unrest-related activity surrounding the administration's immigration policy significantly escalated after ICE agents shot and killed two individuals during operations throughout January, while US military operations against Iran and Venezuela, alongside persistent territorial ambitions over Greenland, have exacerbated anti-war / anti-imperialist sentiments and the broader terror-threat landscape.

Extreme political rhetoric is also being driven by the administration's attempts to amend birthright citizenship and electoral processes, including the Safeguard American Voter Eligibility (SAVE) Act, which would require documentary proof of citizenship to register for federal elections, measures intended to prevent fraud often associated with mail-in voting, and electoral redistricting. Opposition groups view these efforts as unconstitutional and as attempts to illegitimately strengthen Trump / the Republican Party's power base. These efforts are facing various legal challenges and have generated significant uncertainty surrounding the November midterm elections.

- Socio-political and geopolitical issues will almost certainly continue to drive political division in the medium term, increasing the frequency and intensity of protest and unrest, terrorism, and associated threat events. November's midterm elections almost certainly have the potential to act as a turning point for increased political division / extremism, particularly if opposition groups believe Trump's efforts to alter voting rules and Republican-led redistricting efforts unfairly (and potentially illegally) altered the results.

- Extreme actions, such as assassinations, acts of sabotage, violence, and serious vandalism, will almost certainly pose a risk to organizations operating in the US. Those directly associated with the current administration or the implementation of controversial policies are most likely to be targeted; however, politically neutral organizations risk experiencing second-order effects.

Significant developments

Date	Location	Description
25 Apr	Washington DC, US	Trump and other senior administration officials were evacuated from the White House Correspondents' Dinner after an armed man attempted to breach the security perimeter outside of the ballroom hosting the dinner.
28 Mar	Los Angeles (LA), US	Protesters clashed with police outside a federal detention center following a protest held as part of an anti-Trump 'No Kings' nationwide day of action. Protesters surrounded the building - some throwing rocks, bottles, and broken concrete blocks - while one spray-painted "kill your local ICE agent" on the building's facade.
12 Mar	West Bloomfield, US	A naturalized US citizen born in Lebanon drove an explosive-laden vehicle into a Jewish Reform synagogue before being fatally shot by security personnel.
15 Jan	Minnesota, US	Trump threatened to invoke the Insurrection Act in Minnesota if the state government did not do more to combat elevated anti-immigration enforcement protest activity sparked by the shooting of two US citizens.

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.

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

The US continues to apply counterterrorism tools, designations, and strategic language to criminal organizations in 2026, extending the ‘War on Terror’ paradigm to drug cartels and other transnational organized crime groups (OCGs), framing them as national-security threats requiring counterterrorism tools, despite their lack of ideological persuasion. This was explicitly confirmed in the 2026 US Counterterrorism Strategy, released on 8 May, which identified transnational gangs as one of the three major types of terror groups, alongside Islamist extremists and violent left-wing extremists. This shift grants access to enhanced legal powers, enabling intelligence, surveillance, and military resources that would not be available if these groups were treated solely as criminal organizations.

This focus has incited diplomatic tensions between the US and various Latin American countries, for instance, upon US President Trump signing a directive to the Pentagon to begin using military force against Latin American drug cartels in August 2025, Mexico’s President, Claudia Sheinbaum, refused the US military, stating that they would cooperate but ruled out an *“invasion.”*

- The reframing of crime through the lens of counterterrorism will almost certainly persist throughout 2026, consistent with US President Donald Trump’s long-standing political priorities, which have repeatedly advocated for a hard-line, preemptive posture with maximum state power. This will likely be used to define the evolving framework for the ‘War on Crime’, justify military powers, and the international intervention against US adversaries. The use or expansion of powers will likely see development as transnational threats arise and persist, highly likely to show escalation where there is a lack of state cooperation.

- There is a realistic possibility that such a hard-line approach to transnational gangs will trigger international geopolitical tensions and geoeconomic confrontation, whereby measures such as tariffs, sanctions, and export limits are used as leverage if countries in the region are deemed non-complicit. The sustained weaponization of economic interdependencies will likely impact supply chain logistics, supply-demand ratios, and existing / prospective commercial relations, incurring financial burdens and operational disruption across various markets.

Significant developments

Date	Location	Description
8 May	Pacific Ocean	The US military conducted strikes against a vessel accused of smuggling drugs in the eastern Pacific, killing two and leaving one survivor, as part of a sustained operation to combat drug smuggling in the region.
6 Mar	Washington DC, US	The US designated two groups, Primeiro Comando da Capital and Comando Vermelho, as terrorist organizations.
3 Mar	Ecuador	Ecuadorian and US military forces launched operations against narco-terrorist organizations as part of a broader effort against criminal networks and drug cartels in Latin America.

Advisory

- Maintain awareness of international geopolitical tensions motivated by the US's approach to criminal gangs, monitoring cooperation, and a possible degradation in relations that could indicate an escalation into economic leverage.
- Map vulnerable supply chain routes and logistics that could be exposed to security threats and operational disruption should geopolitical tensions rise, ensuring domestic alternatives are available.
- Consult with third-party and vendor organizations to develop robust contingency plans in the event of unrest.


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

Europe

5

Civilian recruitment alters the threat landscape across Europe

The trend of hostile actors increasingly leveraging civilians, both unwittingly and deliberately, to advance their strategic objectives in European states has accelerated and gained significant attention from security services across Europe and the media over the last six months due to the emergence of the Iran-aligned Harakat Ashab al-Yamin al-Islamiyya (HAYI) in March. The group has claimed responsibility for a series of attacks against symbolic 'soft-targets' associated with Israel or the Jewish communities across Europe (primarily in Belgium, the Netherlands, and the UK), triggering various national authorities to implement responsive measures such as deploying military personnel, increasing surveillance of suspected targets, and altering their intelligence posture.

While the composition of HAYI's internal structure remains highly ambiguous due to the lack of credible information regarding its membership and leadership, the group regularly disseminates propaganda across various online platforms following attacks, which likely has a partial aim of attempting to radicalize elements of Western society that are sympathetic to Iran and encourage self-initiated attacks. It is further suspected of recruiting civilians to carry out attacks.

HAYI's emergence occurred against a backdrop of both Russia and Ukraine accusing each other of recruiting civilians to carry out acts of gray-zone warfare (GZW), such as arson and planting improvised explosive devices (IEDs), and organized crime groups (OCGs) across Western Europe continuing to use underage individuals to carry out illegal activities, highlighting the sustained diversification of the threat landscape influenced by state and non-state backed threat actors.

- 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 in the near-to-medium term and be exacerbated by the growing presence of propaganda, terrorist material, and instructional manuals on open-source platforms.
- For organizations, this trend will likely lead to an increase in hostile reconnaissance, sabotage, and targeted attacks that will be increasingly difficult for authorities to detect, prevent, or attribute, necessitating enhanced surveillance capabilities and protective measures.

Significant developments

Date	Location	Description
23 Apr	Amsterdam, Netherlands	Dutch intelligence warned that state actors are increasingly using criminal networks and individuals for espionage purposes in its annual report.
9 Mar	Liège, Belgium	An IED was detonated outside a synagogue, marking the first in a series of targeted attacks claimed by HAYI.
26 Jan	Stockholm, Sweden	The government announced plans to lower the age of criminal responsibility from 15 to 13 on 1 July as part of broader reforms aimed at addressing the country's rising crime rate.

Advisory

- Enhance threat detection and security protocols at sensitive sites, including strengthened site 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.

Anti-migration sentiments elevate across Europe

While current and projected statistics suggest that migration rates into Europe will be lower than those of 2025, anti-migration sentiments have continued into 2026, characterized by an ongoing yet fragmented shift from reactive and crisis-driven anti-migrant protests and rhetoric in previous years towards right-wing policies and regulations. Political coordination for anti-migration sentiment has increased across Europe, focusing on sovereignty, enforcement, and EU overreach, amplifying far-right narratives and power, and decreasing strategic reliance on street-level mobilization; their increased presence in parliaments, governments, and EU-level alliances provides a more legitimate, visible, and effective platform to advance the sentiment. This has effectively normalized anti-migration narratives and politics from the outskirts of political discourse.

- Anti-migration sentiment across the EU will likely continue to increase, reflected in democratic positions, such as local / regional councils, government, and parliaments. This will likely inspire a broader and more sustained policy and regulation transition across the EU, with individual countries likely to mirror such sentiment. Significant increases / spikes in migration rates will likely incite a hardened political stance across various countries, notably those pressured by far-right mobilizations, but it is highly unlikely to eliminate incidents of violent attacks and hate crimes attributed to the movement.

- Despite a decreased physical security threat from right-wing mobilizations, the political shift towards right-wing goals will likely see an increase in tighter work-permit rules and residency restrictions, possibly posing a recruitment challenge. This will likely necessitate a change to internal procedures to prevent later issues during employment; however, there is a realistic possibility that this will incite criticism about public-private relations. A broad transition to a right-leaning political stance across the EU will likely see an increase in protectionist policies, reducing EU integration, strengthening border controls, and pushing national-first procurement policies. This has a realistic possibility of disrupting supply chains, cross-border logistics, and investment flows.

Significant developments

Date	Location	Description
7 May	Nationwide, UK	The right-wing UK Reform Party gained the most seats in the most recent local elections, marking a significant increase in the party's local influence and political momentum.
26 Feb	EU-wide	The European Commission warned of an increasingly violent far-right extremist narrative across the bloc, defined by greater online radicalization and transnational networking.
10 Feb	EU-wide	The EU implemented fast track asylum rejections, expanded safe third country transfers, mandatory border procedures, and tougher deportation rules, championed by right-wing lawmakers.
8 Jan	Helsinki, Finland	Finland made amendments to its Aliens Act, raising the income requirement for family reunification and restricting access to social benefits for new migrants.

Advisory

- Ensure workplace welfare support is in place for those who need it across all operations, allowing third-party and vendor organizations access where appropriate to support the proper integration of migrants into organizations, considering local and regional regulations.
- Maintain awareness of possible flashpoints for far-right activism; despite decreasing, sudden political shifts away from the right, or a spike in migration, could inspire mobilizations that require enhanced security measures surrounding operations and assets.
- Avoid involvement in industry-wide political controversies, notably where migration is involved.

European governments under financial pressure amid economic transition

Numerous European countries continue to face notable 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. In many cases, pressures that existed at the end of 2025, such as political and economic tensions between European countries and China, efforts to further decouple from Russia's natural resources, the ongoing rise in protectionist economic policies, and the US's volatile economic policy, have been exacerbated by the closure of the Strait of Hormuz throughout the ongoing Iran conflict, worsening the overall outlook.

Economic conditions continue to instigate / contribute to political issues in various countries across the region. Notably in France, political and economic uncertainty caused by opposition to planned fiscal cuts continued to present a hurdle to passing the 2026 budget until a significant compromise was finalized in February. Likewise, the Romanian government collapsed on 5 May amid efforts to implement a series of reforms aimed at reducing the country's fiscal deficit and securing access to significant EU funding.

- While geopolitical developments almost certainly have the potential to influence economic conditions across Europe, macroeconomic conditions are highly unlikely to experience significant changes over a short time period. Instead, it is probable that European governments will continue to face fiscal pressures and the associated political challenges while planned reforms / mitigation strategies are implemented and given time to alter market conditions.

- Weakened economic forecasts and other fiscal pressures are highly likely to influence procurement and investment strategies of organizations operating across the public and private sectors, likely encouraging a cost-sensitive and risk-averse approach. While industries identified as probable vehicles for economic growth or important for the national interest are likely to be relatively isolated, this is highly likely to impact organizations operating across the region.

Significant developments

Date	Location	Description
5 May	Romania	The Romanian government collapsed amid efforts to implement fiscal reforms aimed at reducing the country's deficit and securing EU funds.
16 Apr	Germany	The German government halved its growth forecast for 2026 and lowered estimates for 2027, while also increasing inflation projections.
1 Jan	Austria	The retirement age for individuals born after 1968 increased to 65.
1 Jan	Germany	The Active Retirement Act came into force, which allows retirees to earn €2,000 per month tax-free, as part of efforts to keep people in the workforce.

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.

Wild cards

Global markets destabilized by AI bubble burst

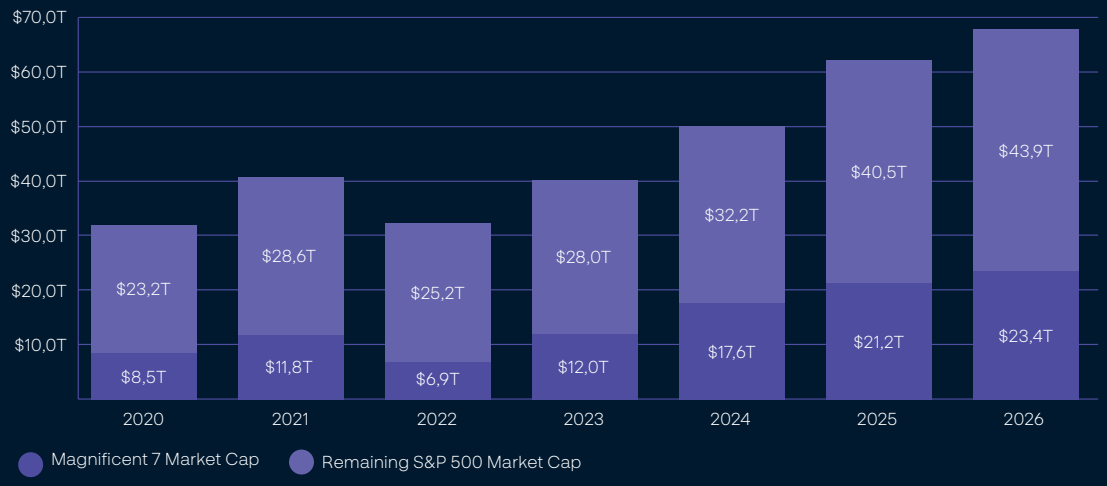
Increasing valuations of companies focused on developing AI and the infrastructure to support it have continued to serve as a primary driver of market growth in 2026, despite the further emergence of investor concerns triggered by additional negative market / industry indicators. The valuation of the 'Magnificent Seven,' a collection of companies associated with AI, namely Alphabet, Amazon, Apple, Meta, Microsoft, Nvidia, and Tesla, increased from ~$19.5 trillion in late 2025 to ~$21.3 trillion at the time of reporting, despite growing doubts surrounding return on investments (ROI) and adoption. This represents ~35% of the S&P 500 index and has been identified as a significant systemic risk by financial institutions such as the Bank of England.

While not a publicly traded company, OpenAI is a significant market actor and is closely entwined with other market leaders. Reports published on 28 April showed the company missed internal revenue targets and that internal projections indicate a ~$14 billion loss in 2026. This was attributed to the failure to achieve its goal of one billion active users for its flagship product ChatGPT, alongside persistent failures to effectively monetize existing users, leading analysts to predict cash shortages as early as mid-2027 without fresh capital. 2026 has further seen OpenAI cancel the planned expansion of their AI data center in Abilene, Texas, over financing disputes with Oracle, and suspend £31 billion of planned investment into the UK's tech sector.

- AI infrastructure investments remaining a substantial share of market value will likely continue to drive financial risk and uncertainty. AI capacity, reliant upon strategic sectors such as semiconductors, has a realistic possibility of plateauing in the short to medium term as world powers – e.g., China, US – implement and change export / import controls. While prominent firms expanding AI infrastructure have met overall revenue targets, adjusted estimates indicate that revenue misses are a realistic possibility in the short to medium term, which have the potential to trigger an increase in stock selloffs.

- Organizations investing in AI infrastructure, or otherwise drawing upon adjacent industries like semiconductors, electronics, and rare earths, are likely to experience fluctuation in financial accounts and supply chain reliability linked to changing supply and demand dynamics. Geopolitical tensions are highly likely to heighten compliance risk around AI-linked exports / imports and foreign-operated AI, risking penalties, fines, and prosecution. Where organizations have commenced strong uptake of AI solutions in day-to-day business operations, a sudden – but unlikely – loss of access to tools would almost certainly disrupt productivity and delivery of services.

The magnificent 7's growing share of the S&P 500



Significant developments

Date	Location	Description
13 May	US	The Philadelphia Semiconductor Index increased 64%, while the S&P 500 rose 17%, from late March to early May. The scale of AI infrastructure stock values drew comparison to the 1999-2000 dot-com bubble.
29 Mar	Global	Valuations in software and semiconductors were noted to be unwinding in a report from Fortune; however, individual AI firm valuations continued to increase, with OpenAI climbing $250 billion in six months.
26 Feb	US	Rare earth shortages reportedly worsened across the US aerospace and semiconductor sectors as export licensing delays and tight Chinese controls continued to restrict access to critical materials such as scandium and yttrium.

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.

Elevated geopolitical competition in the Arctic region

Geopolitical competition in the Arctic has significantly increased in 2026, driven by climate change, energy insecurity, military expansion, economic incentives, and weakened governance, making the region a major strategic asset for world powers to assert influence and control. In early January, US President Donald Trump asserted that the US needed to possess Greenland for national security purposes, with Trump citing Chinese and Russian activity in the region and senior administration officials indicating military options were being considered. This triggered a significant diplomatic dispute with the EU, several NATO countries, and other Danish allies, which caused tariff threats, disrupted the implementation of the EU-US trade deal, and prompted increased military deployments and further investments in Arctic security, while undermining trust and assumptions about the regional threat landscape.

As climate change worsens, ice melt opens new shipping routes and expands access to resources at a time when global energy insecurity and supply chain competition make such access strategically urgent. A continued breakdown in the Arctic Council's governance has exposed the region to further vulnerabilities, stunting the sharing of intelligence, coordinated environmental protection, and offensive mediation.

- Competition across the Arctic region is almost certain to continue to elevate throughout 2026, shaped by long-term, mutually reinforcing structural drivers that are currently operating under fragmented governance. With no current indicators of resolve, the current dynamics between the involved nation-states are likely to further degrade, likely increasing the possibility of further military postures and security concerns.

- Dynamics are almost certain to fluctuate, with shifting power and authority likely creating a highly uncertain and ambiguous environment for negotiation and cooperation, which has the realistic possibility to inspire trade-related retaliation. This could include the controlled use of shipping routes, or, in the case of a significant escalation, broader geoeconomic confrontation used as leverage in discussions, which would likely have an indiscriminate impact across various sectors.

Significant developments

Date	Location	Description
12 May	Greenland	The US has been holding regular negotiations with Denmark to expand its military presence in Greenland to allow the surveillance of potential Russian and Chinese maritime activity.
20 Mar	Arctic region	Russia is allegedly creating a new military communications system to form a mobile field network designed to enable troop command and control, data transmission, and operational coordination.
14 Feb	North Atlantic and High North	The UK announced plans to deploy a carrier strike group to the North Atlantic and High North in 2026, citing increasing regional insecurity.
11 Feb	Arctic and High North region	NATO launched a multi-domain Enhanced Vigilance Activity (eVA) called Arctic Sentry to strengthen security and deterrence.

Advisory

- Map supply chain vulnerabilities that could be exposed by uncertainty in the Arctic region, and create incident response plans (IRPs) should competition impact markets, such as the onshoring of manufacturing.
- Maintain awareness of hybrid threats in the region, such as gray-zone warfare (GZW), that could impact broader aspects, such as cybersecurity and power stability, in areas of operations / logistics.
- Monitor the relations between nation-states involved for possible fiscal repercussions.

Space domain elevates threats to national security and the private sector

The US Space Force identified ~900 attempted cyber intrusions targeting allied satellite operators in Q1 2026, whilst the National Security Agency (NSA), Australian Signals Directorate, Canadian Centre for Cyber Security, and New Zealand National Cyber Security Centre (NCSC) published a statement on 24 March, noting a rising threat landscape towards low-earth orbit (LEO) satellite constellations.

Confirmation of Russia's ''nesting doll' sub-satellite system in April 2026 raised further concerns over anti-satellite (ASAT) maneuvers, including high-velocity projectiles, against LEO satellites and reconnaissance systems. Solar Cycle 25 has also contributed to satellite disruption and early retirement of assets as a greater-than-expected number of X-class solar flares were recorded, causing atmospheric drag and orbital decay.

- Cyber attacks against satellite infrastructure will almost certainly persist, with disruption to global navigational systems, telecommunications, and / or remote internet access remaining likely.

Geopolitical tensions have a realistic possibility of exacerbating the threat posed by ASAT technology, resulting in increasingly frequent attempts to destabilize or neutralize LEO satellites linked to adversarial states. Given sustained high levels of geomagnetic activity early on in 2026, it cannot be ruled out that solar flares demonstrate unexpected, significant intensity as the 12 August 2026 solar maximum approaches.

- Cyber and physical threats to satellites almost certainly have the potential to disrupt navigation, communications, and data services that many organizations rely on, causing immediate operational disruptions. These disruptions can translate into financial losses through penalties, downtime, emergency recovery costs, and rising insurance premiums. Organizations are also likely to face long-term expenses as they invest in resilience measures and navigate regulatory or contractual fallout from service interruptions.

Significant developments

Date	Location	Description
9 Mar	Bet Shemesh, Israel	Hezbollah targeted the Emeq Ha'ela (Ha'Ela) satellite communication station, causing structural damage and destroying multiple smaller antennas.
2 Jan	Paris, France	The European Space Agency (ESA) confirmed a cyber security breach impacting external scientific and engineering servers, with sensitive mission data, credentials, and contractor files stolen.

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.


ÖZEL GÜVENLİK
Securitas

Visit our website
to learn more

Contact

intelligence.solutions@securitas.com