Securitas

Risk Intelligence Center

Annual Intelligence Estimate 2025

ä

January 2025

Intelligence@securitas.com

Contents

Securitas

01

Methodology

A changing world and the ever-changing threat landscape.

***Unprecedented* is a word that has become a primary descriptor for threat and risk in recent years. By its very definition, for something to be unprecedented it has never happened before.**

However, a look back at the last 25 years to 2020 and the turn of the century, tells a different story.

Conflicts, crime, cyberattacks, disorder, espionage, geopolitics, health security, industrial / infrastructure incidents, natural disasters, sabotage – a major world event in each category has happened more than once in this period.

And history repeats itself.

So, while the scale, severity, sophistication and speed of the threat landscape and the risks it poses is increasing, perhaps unprecedented is misleading.

We cannot rule out the unprecedented, the black swans, the one in a millions, the 'most dangerous course of action' (MDCOA).

But what is more realistic is the rise in the *unconventional*: something that is not generally done or accepted.

This is evident in the increase in geopolitical tensions, gray zone warfare (GZW), the AI arms race, increase in insider threats, 'salad bar' extremism, and an increase in private sector organizations finding themselves a casualty in a military conflict they are not directly involved in.

2025 is a flashpoint for the unconventional.

But unconventional is as much about disruption and not following the norm or rules, as it is about creativity and innovation.

This theme is core to the 2025 Annual Intelligence Estimate.

What is the RIC's Annual Intelligence Estimate 2025?

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

The Annual Intelligence Estimate includes a selection of corporate security issues, and key geographic considerations. The report is intended as an actionable alternative to other thematic assessments, with security decision makers in mind. It provides situational awareness for organizations in all industries and sectors, and as such is produced as a digestible high-level brief for a general audience complete with practical considerations.

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

Approach

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

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

Threat levels

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

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

Language of probability

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

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

Intelligence Cut Off Date (ICOD):	0000hrs UTC 01 January 2025

Trends, patterns, and influencing factors

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

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

2023	2024	2025
ESG initiatives incite backlash and security threats	Convergence of geopolitical and sociopolitical threat actor motivations	Changing 'rules-based order' heightens concerns over possible collapse
Chronic stresses of climate change and the acute shocks of natural disasters	Chokepoints and great power competition disrupt supply chains	Heightened gray zone warfare and sabotage threaten organizations' security
Balancing health security versus hypersensitivity	2024 super election cycle	Organizations increase preparations for 'wartime scenarios'
The ever-evolving cyber threat landscape	Artificial intelligence arms race	Executives and politicians in the crosshairs of threat actors
Information disorder and the increasing real-world threat of 'fake news'	Climate and environmental risks reach new limits	AI faces its watershed moment
The expanding activist landscape	Supercharged cybercrime	Ideological insiders increasingly threaten organization security
(R)evolution in terrorism and extremism	Global impacts of China's economic downturn	The growing overlap in threat actor motivations
Espionage targeting organizations and their assets	ESG backlash turns from bark to bite	Exploitation of drones for hostile purposes
Energy resilience and security	Critical infrastructure to remain a critical vulnerability	Social media exploitation fuels information disorder
Threats to global supply chain resilience and security	Increasing corporate espionage shifts focus to counter-intelligence	Impacts of health security events ripple across supply chains

The influence of Strategic Drivers on the global security threat landscape – PESTLE analysis

	Strategic Drivers identified in 2024	Expected Strategic Drivers in 2025
Political	▪ The **2024 'super election cycle'** played a key role in shaping domestic, regional, and global political landscapes, with right-wing parties / figures gaining increased popularity. ▪ **Global conflicts** influenced many countries' foreign policy, geopolitical relations / tensions, and domestic unrest – including outside impacted regions. ▪ **Domestic political instability** across many countries fueled an uptick in civil unrest and violent incidents, including mass casualty events.	▪ Rising **anti-West sentiments** and **political polarizations** in the West are likely to heavily influence domestic, regional, and global politics, driven by the return of the Trump administration in the US. ▪ **Country / regional instability** (largely fueled by conflicts) will continue to involve international powers and influence domestic politics and security in 'unaffected' nations. ▪ Growing **cooperation and expansion of alliances**, such as BRICS, is likely to further impact the influence of Western alliances, such as NATO, heightening security concerns.
Economic	▪ The focus on **diversifying supply chains** increased significantly in line with deteriorating geopolitical tensions, impacting many countries' economies. ▪ **Inflation rates** remained heightened in many countries, causing economic degradation and domestic tensions in impacted countries. ▪ **Unemployment rates** remained below pre-pandemic levels, with many countries seeking to grow and diversify workforces to meet operational demands.	▪ **Foreign trade policies** are likely to be tightened due to geopolitical tensions impacting exports / imports, causing supply chain disruption, increased costs, and influencing investor confidence. ▪ **Diversified supply chains** due to growing industry demands and geopolitical tensions will likely improve the economies of many countries chiefly those associated with tech and manufacturing. ▪ **Global consumer spending is largely** expected to grow steadily, driven by lower interest and inflation rates, though local economies will vary by country-specific conditions.
Sociological	▪ **Social divides** driven by political changes and global conflicts increased domestic and regional unrest, resulting in prolonged outbreaks of violence in many countries / regions. ▪ **Mass displacement** caused by conflicts and climate crises continued to increase causing discontent among various populations and strain on aid systems globally. ▪ **Aging and rapidly growing populations** caused concerns for the immediate and long-term futures of many countries, including their economies and security.	▪ **Move away from liberal views**, driven by economic and social frustrations, fueling information disorder, prompting movements aiming to influence domestic and international politics. ▪ **Migration** continuing to be a key issue at the forefront of many countries' domestic security concerns, with overwhelmed borders and immigration systems expected. ▪ **Humanitarian crises** influenced by food and energy insecurity prompt increased heath threats, further impacted by climate disasters and domestic / regional conflicts.
Technological	▪ The **race to develop artificial intelligence** (AI) improved many countries and organizations' abilities to utilize the technology but has also influenced its exploitation and subsequent security risks. ▪ Increasingly frequent, complex, and damaging **cyber security threats** posed a heightened threat to the public and private sectors. ▪ The race to **diversify technology supply chains** to align with geopolitical rivalries, primarily semiconductors.	▪ The **militarization of AI** is highly likely to be exploited and weaponized by state and non-state-backed threat actors, including by militaries globally, prompting ethical and security concerns. ▪ Vulnerability exploitation and **cyber attacks targeting critical national infrastructure** threaten domestic and international security, with the targeting of private organizations expected to rise. ▪ A **new 'space race'** will further heighten technology competition between nations, with private organizations likely to experience more opportunities, however, risks are also expected.
Legal	▪ The **changing 'rules-based order'** observed reduced compliance of state and non-state actors with legal and accepted norms. ▪ The increasing use of **international sanctions regimes** impacting geopolitical tensions and business operations globally. ▪ **Regulations surrounding emerging sectors**, primarily technology, failing to make significant progress, heightening concerns over expected future threats.	▪ **Global governance structures facing increased push-back** and non-compliance, influencing breakdowns and violations of international laws. ▪ **Lacking regulation of high-risk technologies**, including AI, will prompt an increase in its exploitation, and raise considerable ethical and security concerns. ▪ **International sanctions regimes expand** to include more countries and industries, posing threat to business operations and travel.
Environmental	▪ **Climate disasters** increased, fueled by climate change, causing significant casualties and infrastructure damage. ▪ **Hotter and wetter climates** impacting some countries' natural resources, hindering economies and organizations' ability to operate. ▪ Concerns surrounding organizations' **environmental footprint and sustainability efforts** influencing scrutiny and targeting.	▪ **Transition to clean energy continues to be stalled**, further influencing the climate crisis and backlash for campaigners, including the targeting of organizations and their executives. ▪ **Extreme weather events and natural disasters increase** in frequency / intensity, posing safety threats to organizations' employees, causing infrastructure damage and supply chain issues. ▪ Organizations perceived to be complicit in the climate crisis will face **heightened threats of legal action**, with more 'successful' legal battles posing financial and reputational repercussions.

Take me to...

Corporate Security

Regional Security - AMEA

Regional Security - Americas

Regional Security – Europe

Securitas

02

Corporate Security

Changing 'rules-based order' heightens concerns over possible collapse

Geopolitical tensions in 2024 have deteriorated the established 'rules-based order', also commonly known as 'liberal international order', leading to significant violations of pre-established norms and the use of gray zone warfare (GZW) tactics and kinetic military operations by several states and non-state actors. Events like the Gaza-Israel conflict and the subsequent regional tensions in the Middle East, and the Russia-Ukraine conflict have observed noteworthy violations of international rules including the UN Charter of 1945 for the use of force. This has been met with concerns over a possible collapse of the 'ruled-based order' as rules are increasingly being ignored / flouted, but also changing as the rules are being rewritten in the context of conflicts, geopolitical tensions, and domestic politics.

- Violations of international norms are not exclusive to military fronts. The China-US trade war and tariffs commenced in 2018 have been judged by the World Trade Organization as violating international trade rules. This has led to increased prices and sanctions for organizations in industries such as heavy metals, electric vehicles, and semiconductors, among others.
- Regional / country-specific conditions are also likely to influence investor confidence in businesses with global operations, with industries such as technology, manufacturing, and logistics, most likely to be impacted by persistent changes to the 'rules-based order' largely fueled by political / geopolitical tensions and global conflicts.
- Violations of the 'rules-based order' threaten are also likely to arisen within the sphere of nuclear weapons with nation states both currently armed with nuclear warfare (China and Russia) capabilities and aspiring to them (Iran and North Korea) will likely continue to pursue weapon advancements despite anti-nuclear agreements, risking a new arms race.

Scenario	Scenario condition	Assessed likelihood
Geopolitical tensions ease resulting in a reduction of hostile political and economic actions that allow for the reestablishment of international law and norms.	Improves	Highly unlikely (10%)
Geopolitical tensions continue to lead to violations of international law and norms, which lead to further degradation of the 'rules based order' system.	Baseline	Unlikely (35%)
Violations of international law increase and spread further from conflict zones, leading to additional trade regulations, deterioration of diplomatic relations, and irregular warfare tactics.	Worsens	Likely / Probable (55%)

- ✓ Reduce reliance on specific regions to diversify trade routes and minimize disruptions caused by geopolitical events.
- ✓ Stay informed on tariffs and sanctions to adapt to regulatory changes and mitigate in case of rapid developments. Ensure adherence to international trade laws to safeguard compliance.
- ✓ Develop contingency plans for disrupted diplomatic relations and invest in geopolitical risk intelligence services to anticipate and respond to developing conflicts.

Indicators

- Further escalation / deterioration of the security landscape in the Middle East, Ukraine, or additional conflict zones.
- Additional tariffs and sanctions announced by leading global powers such as China or the US.
- Disregard of resolutions and votes by the UN and associated institutions.
- Victory of nationalistic, isolationist, and Eurosceptic parties and candidates across elections globally.
- Overturn of political systems in favor of authoritarian regimes.

Implications

- It is highly likely that further trade restrictions will be implemented, disrupting supply chains, and increasing regional prices.
- Kinetic military operations and GZW will impact further civilian targets previously considered beyond limits (e.g. commercial airports) leading to associated disruptions to business operations.
- Deterioration of diplomatic relations among pre-existent partners is possible, obstructing employees' travel and bilateral trade.
- New opportunities will arise for countries in the global south previously ignored by the international system.

Heightened gray-zone warfare and sabotage threaten organizations' security

The use of hostile strategies / tactics by state and non-state actors when opposing actors are not engaged in traditional conflict or open war – but peace is also not being observed – known as gray-zone warfare (GZW), is an evolving threat that is increasingly being utilized by a diverse range of threat actors as geopolitical tensions increase. GZW targets often includes military sites, transportation nodes (airports, roads, ports), logistics facilities, government services, and utility infrastructure (energy, water, undersea cables). GZW and sabotage are increasingly likely to result in significant disruption, including mass casualty incidents, supply chain disruption, IT / communications outages, impacting critical national infrastructure (CNI), industries, businesses, and individuals.

- GZW tactics, techniques, and procedures (TTPs) are utilized by a range of nations including, China, Iran, Russia, North Korea, and the US, and can be used in the physical and cyber domains. GZW operations are characterized by not meeting the threshold to incite armed conflict, allowing the perpetrator to threaten / manage escalation, and being strategically ambiguous.
- TTPs include but are not limited to sabotage, sanctions, cyber attacks (against civilian / private sector targets), election interference, electronic warfare, and covert operations. The use of such TTPs is highly likely to continue to be deployed by state and non-state actors fueled by flashpoints in geopolitics, global conflicts, and growing economic competition.
- The direct and indirect targeting of private organizations by GZW is becoming increasingly common, with incidents highly likely to increase in frequency and impact as TTPs become more complex and tensions persist globally.

Scenario	Scenario condition	Assessed likelihood
Heightened security measures implemented by authorities globally decrease the effectiveness of GZW campaigns, limiting the disruption to public life and businesses.	Improves	Highly unlikely (15%)
Threat actors continue to increasingly utilize GZW tactics against a range of Government and private sector targets, causing operational disruption and security breaches.	Baseline	Realistic / Possible (45%)
Threat actors escalate GZW campaigns, adopting increasingly radical TTPs against a broader range of Government and private sector targets, posing significant security threats.	Worsens	Realistic / Possible (40%)

- ✓ Assess exposure to scenario-based threats in the context of organizations, including direct (i.e. targeting by most likely threat actors and their motivation, intent, and capability) and indirect targeting (i.e. impacts arising from loss of key services / infrastructure).
- ✓ Proactively monitor for potential escalations. Utilize intelligence capabilities to assess and monitor threats during heightened periods of threat / unrest.
- ✓ Utilize accurate sources of information and seek to identify and avoid misinformation and disinformation. Consider sharing reliable sources with employees to avoid unnecessary panic from misreporting.

Indicators

- Increasingly frequent high-profile instances of suspicious accidents (fires / infrastructure damage, etc) impacting CNI and sensitive sites.
- Governments increasing terror threat levels, issuing warnings about hostile GZW / sabotage / hybrid action campaigns.
- Governments allocate additional resources to domestic security services and provide training to the private sector.
- Heightened observance of cyber threat activities from state and state-backed cyber threat actors, primarily China, Russia, and North Korea targeting government and private organizations.

Implications

- Private organizations operations are increasingly disrupted and security compromised, particularly those operating CNI or in sensitive industries such as defense.
- States are encouraged to allocate additional resources to their security forces and implement training to raise awareness / increase resilience to GZW operations.
- Threat actors increasingly exploit divisive social issues as part of GZW operations to cause unrest and undermine political systems and government institutions.
- Organizations forced to heighten security measures (cyber and physical) to combat rising threats.

Organizations increase preparations for ‘wartime scenarios’

Organizations are increasingly preparing for ‘wartime scenarios’ due to geopolitical competition, frequent sabotage, and other gray-zone warfare (GZW) incidents, and threats of global conflict surrounding flashpoints such as Gaza, Taiwan, and Ukraine. Numerous countries have increased defense spending, committed to collaborative readiness projects, and shifted to a ‘wartime mindset’, including NATO. Businesses and organizations are increasingly facing the heightened threat of being targeted directly as well as by secondary / tertiary impacts of state-backed action.

- Organizations are increasingly being caught in the crossfire of state-level conflict and disputes, including waves of both economic and diplomatic sanctions issued targeting businesses of adversarial nations, exemplified by Russia listing US cyber security firm Recorded Future as an *“undesirable”* organization in December for allegedly participating in Western propaganda.
- In response to logistical and supply chain vulnerabilities exposed in recent years, certain states have diversified their energy supply, namely moving away from Russian gas, and have also acted to reduce their dependence on China as a primary source of critical materials, as exemplified by the Jadar Valley lithium mine project in Serbia.
- This coincides with increasing warnings from NATO, with its military committee chairman stating civilians must prepare for full-scale conflict with Russia in the next 20 years and urging European businesses to prepare for a *“wartime scenario”*. Civil measures have also been introduced to mitigate the adverse impacts of future conflicts, such as Germany identifying buildings as potential public bunkers, Sweden issuing advice in the case of *“crisis or war,”* and similar guidance in Denmark, Finland, and Norway.

Scenario	Scenario condition	Assessed likelihood
Corporate security improves as relations with China progress and the Russia-Ukraine / Middle East conflicts deescalate, allowing for ‘peacetime’ discourse.	Improves	Highly unlikely (15%)
Relations with China remain tense, and the Russia-Ukraine conflict continues, motivating organizations to maintain increase security postures and resilience measures to prepare for ‘wartime scenarios.’	Baseline	Likely / probable (75%)
Global relations significantly worsen, leading to direct and violent targeting of organizations’ people, property, and assets, along significant secondary and tertiary disruption to CNI and IT.	Worsens	Highly unlikely (10%)

- ✓ Organizations, especially those operating within commonly targeted sectors, are advised to raise employee awareness of potential threats and simultaneously improve their security posture.
- ✓ Organizations are advised to ensure they are not engaging in business or communicating with businesses or assets as they could be exposed to OPSEC risks and domestic scrutiny.
- ✓ Organizations should consider developing and regularly reviewing risk management plans to be deployed in the event of conflict escalation.

Indicators

- State actors such China and Russia are increasingly implicated in GZW operations targeting businesses and organizations.
- World powers continue to increase defense spending, announce new joint defense projects, and warn of ‘wartime measures.’
- Governments issue new civil guidance regarding preventative measures that can be taken ahead of military conflict.
- Private sector organizations develop security and resilience capabilities in line with government guidance.
- Governments continue to encourage businesses to diversify supply chains from adversarial states.

Implications

- Relations with businesses in adversarial states such as China and Russia (and their partners) deteriorate, forcing operational challenges.
- Supply chains and sources of critical materials / essential commodities are diversified, presenting new commercial opportunities, but also likely increased costs.
- Businesses and public institutions are required to improve their security postures, especially in relation to cyber threats, inciting increased financial costs.
- Uncertainty surrounding armed conflict undermines global investor confidence, reducing foreign investment.

Executives and politicians in the crosshairs of threat actors

Increasing threats to organization executives have consistently correlated with workplace grievances and ideological / activist causes, with recent violent incidents highlighting the current heightened threat actor motivation and capabilities to cause physical harm to executives, which is expected to persist into 2025. The threat of high-profile individuals, such as senior executives and politicians, being targeted by malicious threat actors has persisted amid ongoing geopolitical tensions with China, Iran, and Russia and their exploitation of global internal divisions via foreign state actors.

- Radical activists and self-initiated threat actors have been observed to increasingly target executives / politicians in support of their cause, including through the use of violence, such as with the assassination of UnitedHealthcare CEO in December and the arson attack targeting Rheinmetall CEO in April.
- The targeting of politicians in 2024 is highly indicative of escalating threats towards political figures, including the attempted assassinations of US President-elect Donald Trump and Slovakian Prime Minister Robert Fico. While mainly consisting of 'self-initiated' attacks, foreign state actor attacks are increasing.
- Non-physical targeting methods include utilizing information disorder, doxing, and malicious communications aimed at causing maximum damage / disruption to the targeted individual or their associated entity. As threat actors enhance their capabilities and utilize increasingly threatening tactics, aided by advancing technologies, such threats are likely to continue to impact executives and politicians on a significant scale.

Scenario	Scenario condition	Assessed likelihood
Attacks against executives decrease, geopolitically-motivated protest activity targets organizations, but without serious targeting of executives / politicians.	Improves	Highly unlikely (10%)
Threat actors continue to use mixed tactics to target executives and politicians, primarily online, but with increasing instances of in-person direct targeting.	Baseline	Realistic / Possible (50%)
More violent tactics increase, including successful assassinations and terror attacks, increasing global security measures around VIPs.	Worsens	Realistic / Possible (40%)

- ✓ Develop security frameworks for VIPs to ensure protection amid increasing risks to life and malicious influence. Carry out the operations security (OPSEC) cycle with a variety of internal stakeholders about the cyber presence of the organization online, including on social media.
- ✓ Malicious or threatening communications should be notified to authorities, with persistent / substantial targeting potentially leading to the implementation of court injunctions or restraints to limit future targeting.
- ✓ Be aware of the potential risks of making public or official statements regarding provocative or controversial actions, as these may be exploited by threat actor groups to engage in hostile or threatening actions.

Indicators

- Increased attempts to assassinate or inflict harm to executives / politicians or other VIPs.
- Changes in security protocols and increased measures for executives / politicians and their associates or assets.
- Persistent advertisement of online campaigns targeting businesses / governments departments related to VIPs, including malicious communications using provided templates.
- Increased reports of politicians being exploited for espionage / agents of influence via honeytraps by foreign state actors.

Implications

- Business operations delayed / canceled due to security precautions amid threats and risk of attacks against VIPs.
- Online services for businesses and government institutions disrupted by cyber attacks or spread of mis / dis / malinformation via social media.
- Businesses' brand reputations damaged and impact on business relations due to threats of targeting within supply chains.
- Businesses / government departments increasing security budgets to match appropriate VIP protection with heightened threat landscape.

AI faces its watershed moment

Artificial intelligence (AI) will continue its rapid evolution in 2025, with its increasing integration in the workplace presenting additional vulnerabilities for threat actors to exploit. As businesses increasingly utilize large language models (LLMs), organizations may inadvertently disclose sensitive data that LLMs can reveal, leading to unauthorized data access and security breaches.

- A proliferation of open-source AI platforms and generative AI is likely to serve as a force multiplier for threat actors, lowering the entry barrier for malicious actors to launch cyber attacks, sow disinformation via deepfakes, or conduct hostile reconnaissance and target selection.
- As the ecological costs behind AI become more well-known, environmental backlash against the technology is likely to increase. This is likely to incite protests targeting specific organizations employing the technology and infrastructure supporting AI such as data centers. Increasing use of AI in the workplace, alongside fears that it will replace jobs, will likely continue to incite backlash. While these protests are likely to gain momentum, fringe activist groups are unlikely to coalesce into global movements and extremism, meaning significant threatening incidents are unlikely in 2025, although these cannot be ruled out.
- Enhanced guidelines and regulations surrounding AI are likely to come into force in 2025, providing governments and businesses greater clarity surrounding the use of the technology. However, these are unlikely to keep pace with the rapid development of AI, meaning threat actors will continue to exploit loopholes. It is also realistic that AI will face constraints of utilization, growth, and development due to energy concerns which have become increasingly prominent on a local and regional level.

Scenario	Scenario condition	Assessed likelihood
Legislative successes, improved AI ethics, and strong security frameworks contribute to widespread benefits and significant public trust in AI systems.	Improves	Highly unlikely (10%)
Rapid adoption of AI increases the likelihood of vulnerabilities exploitable by threat actors while improving their capabilities. For organizations, a 'burst bubble' leads to managed expectations regarding what AI can and cannot achieve, and an increase in protests against the use of AI over its environmental impacts.	Baseline	Likely / Probable (65%)
Threat actors utilize generative AI to launch multiple hyper-personalized social engineering attacks, while terrorists leverage AI to launch significant attacks, potentially including CBRN materials.	Worsens	Unlikely (25%)

- ✓ Ensure all personnel, as well as third parties, are informed and up to date on legal / regulatory requirements regarding AI, especially regarding potential differences in legislation in different countries, to avoid financial or legal repercussions.
- ✓ Train executive teams in detecting AI-driven impersonation tactics, such as deepfake call or spear-fishing attempts.
- ✓ Establish AI content authenticity and verification systems, and verify the sources and credibility of information before use – internally and externally.

Indicators

- Growing disillusionment with certain AI technologies and their return on investment.
- Increased use of AI for hostile purposes, such as cyber attacks and disinformation campaigns.
- Accelerated development and adoption of AI tools with new or improved capabilities.
- Uptick in insider threat cases where disgruntled / vulnerable employees are targeted by AI-generated messages.
- Shift in executive rhetoric from AI being the 'future of all processes' to a more balanced perspective that emphasizes caution.

Implications

- New regulations for AI impacting businesses, with potential for operational, compliance, and legal issues.
- Targeting of organizations with links to AI by threat actors (activists, competitors, cyber threat actors, extremists, state-backed entities) resulting in disruption.
- Organizations are likely to require increased security budgets to address advanced AI-enabled threats.
- Increased number of successful cyber attacks utilizing AI exploiting existing vulnerabilities causing significant security breaches and data leaks, inflicting legal and financial challenges for impacted organizations and supply chains.

Ideological insiders increasingly threaten organizations’ security

Ideologically motivated insider threats have become increasingly common as widely popular activist causes, personal grievances, and political differences have motivated employees to target organizations and supply chains. Major flashpoints in activism, ranging from geopolitical tensions to environmental causes, have greatly contributed to the growth of activist movements, which have been increasingly recruiting employees to target their organizations, with this trend likely to continue into 2025.

- Malicious threat actors are likely to see any involvement in organizational practices or activities contrary to their beliefs as a legitimate motive for targeting. Critical industries such as defense, aerospace, technology, infrastructure, and biotech are at a higher threat of targeting by state-sponsored threat actors.
- The popularity of ideological causes and controversies in social discourse is highly likely to influence ideologically driven insider threats, especially in the West. Whistle-blowing, walkouts, sabotage, disruptions to operations, leakage of sensitive data and internal communications as well as attempts to negatively impact an organization’s brand image and reputation are all tactics, techniques, and procedures that are likely to continue to feature in ideologically motivated insider threat-related incidents.
- Insider threats can be harder to prevent and potentially more dangerous as the threat actors have a deeper knowledge of the target organization and are aware of their vulnerabilities. The expected persistence of the ongoing ‘insider threat crisis,’ the potential for the emergence of new flashpoints, and the increasing influence of global activism are highly likely to continue pose a complex threat to organizations in all sectors.

Scenario	Scenario condition	Assessed likelihood
Common workplace dispute causes (wages, unfair dismissals) decline in frequency, paired with a resolution of ongoing flashpoints leading to a reduction in ideological insider threats.	Improves	Unlikely (30%)
Malicious insiders continue to exploit organizational vulnerabilities in association with workplace grievances and their ideological causes, causing data leaks, security threats, and operational disruption.	Baseline	Likely / Probable (50%)
Divisive ideological discourse increases with violence and terror-related activities becoming an increasingly deployed tactic by ideologically motivated insider threats.	Worsens	Highly unlikely (20%)

- ✓ Organizations are advised to develop effective insider threat identification and detection programs, focusing on behavioral indicators / exploitable traits, repeated security violations, and unnecessary attempts to become involved in sensitive or restricted areas, combining human resources and technology.
- ✓ Organizations should maintain situational awareness to pre-emptively identify issues or trends that may see an increase in insider threats, whether targeting the organization specifically, its partners, or the supply chain.
- ✓ Ensure employees are aware of reporting procedures for suspicious behavior and activity within the workplace.

Indicators

- Employee groups, unions, or individuals voice politically motivated disagreement with their organization’s operational practices / policies.
- Ongoing popular flashpoints for activism continue to target private organizations and subsequently act as motivation for ideological insider threats.
- Threat actors maintain social media campaigns, outreach, and calls to action directed at individuals employed by target organizations.
- Employees engaging or promoting activist / ideological content on social media, including material critical of their employer.

Implications

- Leakage of sensitive data by insider threats posing security threats, including within supply chains, and possible reputational damage.
- Potential for individuals / groups of like-minded ideologically driven employees to disrupt daily operations or sabotage their workplace.
- Reputational threat stemming from employees publicly criticizing their organization.
- Potential cost of increased security and monitoring measures within the organization to identify and prevent insider threat disruptions.
- Possible use of violent tactics is likely to result in casualties, posing security threats to the workforce.

The growing overlap in threat actor motivations

The motivations of hostile threat actors worldwide have become increasingly intertwined as geopolitical issues have become more prevalent domestically, and domestic socio-political grievances have been felt internationally, blurring the lines between both groups and tactics. This is likely to result in a more varied array of threat actor networks driven by new and divergent grievances with a wider perception of viable targets and means of launching attacks.

- Highly motivated activist groups and individual activists have shifted from non-violent direct action and generic protest tactics to more radical / 'extreme' tactics, aiming not only to raise awareness but also to cause material disruption, permanent damage, and safety and security threats to senior executives. This has also influenced a rise in violent and terror-related incidents.
- Both geopolitically and socio-politically-motivated groups have escalated to destructive and violent direct action targeting businesses, buildings, operations, and personnel linked to global concerns – including conflicts – in addition to increasing 'militarization' of other activist causes, such as climate activism.
- As the motivations of threat actor groups increasingly overlap, different threat actor groups are likely to carry out actions coordinated across movements and even borders, forming global campaigns made of national actor groups spread across international umbrella organizations, multiplying their ability to target organizations and executives.
- Larger cross-motivation and cross-border threat groups are likely to increasingly develop sophisticated tactics, techniques, and procedures (TTPs) shared across motivations, including 'extreme' TTPs threatening people, property, and operations.

Scenario	Scenario condition	Assessed likelihood
Overlap of motivations reduces and does not result in blurred lines with extremist groups, promoting peaceful and non-violent campaigns.	Improves	Highly unlikely (10%)
Threat actor groups, particularly activists, increasingly overlap on geopolitical and socio-political issues, sharing coordinated tactics with target lists, motivated by multiple socio-political grievances.	Baseline	Likely / Probable (55%)
Radical and extremist actors are borne from cross-motivation activist flashpoints, normalizing serious, legitimate, and coordinated threats to businesses in socio-political controversies.	Worsens	Unlikely (35%)

- ✓ Assess exposure to international and domestic issues that drive threat actor grievances, including through business practices, contracts, partnerships, and subsidiaries.
- ✓ Monitor for warnings of threat actors who may be incited / influenced / inspired to take action with the potential to cause business impact (directly or indirectly), stemming from the business landscape and reputational footprint.
- ✓ Develop and maintain scenario-specific incident response plans for coordinated threats, integrating security protocols with people, property, operations, and reputation.

Indicators

- Increased support and coordination between threat actor networks worldwide on open source and in-person.
- Flashpoints of increased threats in response to significant current events (both international and domestic) and planned events (i.e. conflicts, elections).
- Increase in information disorder, including concerning real-world events, or fake events, and their links to organizations.
- Normalization of more radical tactics internationally, including violence.
- Increased focus and 'blame' on organizations over controversial issues and activities.

Implications

- A more varied array of threat actors driven by new and divergent grievances with a wider perception of viable targets and means of launching attacks.
- Increase in threats reacting to both local and international current events, raising opportunities for cross-movement support and targeting.
- Increase in brand and reputational threats related to conflicts, climate change, socio-economic issues, and environmental, social, governance (ESG).
- Increase in targeting of organizations and specific personnel (i.e. executives) associated with controversial topics.

Exploitation of drones for hostile purposes

Technological advancements in drone technology continue to present opportunities for threat actors, including activists, criminals, and terrorists who can exploit drones – civilian, commercial, and military – for a variety of activities, including offensive purposes, hostile reconnaissance, and publicity, as well as weaponizing drone to undertake attacks. Civilian drones are available to members of the public, do not require a license to buy or operate, and are reasonably priced, allowing threat actors to attain drones without significant capability or financial resources. Increased reporting of drone sightings over sensitive sites and private organizations has raised concerns over possible malicious and accidental impacts on targeted entities, including sites / assets of private organizations.

- While drone regulations globally likely vary, drones remain capable assets for threat actors to conduct malicious activities. Exploitation of civilian drone regulations likely allows drone operators to fly over residential, recreational, commercial, and industrial sites, using the integrated camera to survey and record sites, making civilian drones perfect for hostile reconnaissance operations. Drones with cameras are valuable devices for recording protests, attacks, or other actions for later publicity on social media.
- As the conflict in Ukraine has demonstrated, civilian drones can also be perfect vehicles for transporting offensive payloads, a tactic that has the potential to be exploited by a range of threat actors. Drones have the potential to be used to breach secure locations using explosives / ramming, targeting people by flying into them, carrying hazardous materials, and generally disrupting sites / causing distraction.

Scenario	Scenario condition	Assessed likelihood
Legal legislation on the use of drones over private and commercial sites is enhanced by requiring applications to attain / fly drones over private or / commercial property.	Improves	Highly unlikely (10%)
Hostile threat actors increasingly access drones with reasonable ease to conduct hostile actions against businesses, including surveillance and damaging infrastructure.	Baseline	Likely / Probable (55%)
Sophisticated drones without regulatory limitations allow threat actors to fly hazardous materials at targets, potentially including explosives, CBRN materials, and weapons.	Worsens	Unlikely (35%)

- ✓ Ensure that site managers are aware of drone legislation in the local area to assess the likelihood of threat actors being able to use drones above the site, especially at sites deemed to be sensitive.
- ✓ Consider the repositioning of CCTV to aid in capturing airborne threats and ensure security teams are advised on how to handle downed drones, especially those that may carry hazardous or explosive materials.
- ✓ Develop clear and effective response plans for drone incidents targeting a site, as well as when drones are observed in the vicinity of sites, including business continuity plans to ensure that the site remains operational and assets are not significantly impacted by drone activities.

Indicators

- Increased use of drones for hostile purposes, such as hostile reconnaissance to prepare for actions targeting sites.
- Continued exploitation of drone legislation and regulations to allow hostile threat actors to freely fly over and film sites from above.
- Elevated incidents of both malicious and non-malicious sightings of drones above organization sites.
- Heightened sales of civilian and commercial drones through legitimate and illegitimate means.

Implications

- Potential disruptions to site operations due to drone activity, especially at sensitive sites.
- Organizations, particularly in sensitive industries, will be required to invest in protection measures to combat drone use, such as alerting systems.
- The ability to differentiate between civilian drones used for non-malicious purposes and hostile threat actor drones will become more difficult as sightings become more common.
- Commercial pressure on governments to change drone regulations to prevent further drone incursions onto organization sites.

Social media exploitation fuels information disorder

There are three main types of information disorder: misinformation, disinformation, and malinformation. As we move into 2025, information disorder is expected to remain a significant threat to organizations, with threat actors continuing to circulate false, misleading, or harmful information primarily related to organizations operations, business partnerships, and their executives. This will particularly be the case in the context of societal, governmental, and geopolitical flashpoints, impacting businesses in various ways including reputational, financial, and operational damage.

- Ongoing geopolitical tensions will likely influence state actors to leverage information disorder to fuel social and political polarization. Social media will remain a key tool for disinformation campaigns, to incite political discord, and destabilize society. These campaigns have the potential to influence public opinion, disrupt democratic processes, and undermine trust in public institutions.
- Threat actors are continuously evolving their tactics to manipulate narratives via social media, often using increasingly sophisticated techniques to drive global discourse and shape societal perceptions, with the involvement of 'high-profile' individuals or officials highly likely to further attention to such discourse and enhance the overall threat.
- Domestically, the use of deepfake technology is expected to grow, with threat actors developing more convincing methods to spread disinformation and evade detection. This will further complicate efforts to identify and combat information disorder main types of information disorder: misinformation, disinformation, and malinformation.

Scenario	Scenario condition	Assessed likelihood
Legislation enhances platform transparency in moderation and algorithms, with stricter laws and penalties targeting information disorder.	Improves	Unlikely (25%)
Threat actors continue to propagate information disorder, leading to disruption based on misleading and false information. Election cycles will remain vulnerable to manipulation due to information disorder.	Baseline	Likely / Probable (55%)
Threat actors continue to exploit social media, leading to distrust in governmental organizations, while societal polarization deepens, contributing to widespread social unrest.	Worsens	Highly unlikely (20%)

- ✓ Ensure that incident response plans are in place and regularly rehearsed to effectively address instances of information disorder, ensuring that official communications are disseminated efficiently to counter false narratives.
- ✓ Consider the reliability and credibility of unofficial sources and social media channels, and utilize recognized fact-checking platforms to identify potential instances of information disorder.
- ✓ Consider employing authentication techniques in public-facing communications, such as digital watermarking, which can be used to verify authenticity.

Indicators

- Significant elections or votes are likely to trigger a surge in information disorder.
- Public health crises spark misinformation campaigns, especially around vaccinations, fueling anti-vaccine movements and undermining public health guidance.
- Media coverage of localized violent crimes often spreads information disorder, vilifying specific ethnic or religious minority groups.
- Rising geopolitical tensions drive state-backed campaigns that spread information disorder.

Implications

- Organizations may face significant reputational harm as misinformation or disinformation campaigns target the brand or executives.
- Rising use of violent tactics targeting high-profile individuals, including organizations' executives, fueled by information disorder is highly likely to pose safety and security threats, including during business travel.
- Rising concerns over information disorder may lead to stricter regulations and compliance requirements, particularly in areas such as data privacy and content transparency.
- Organizations may be required to invest in crisis management resources to monitor, identify, and respond to instances of misinformation campaigns.

Impacts of health security events ripple across supply chains

Considering the global impact of the COVID-19 pandemic, the spread of recent infectious diseases such as mpox and bird flu has caused widespread alarm in corporate organizations, with governments largely acting quickly in response to localized outbreaks to minimize impacts. Questions remain over the ability of governments and businesses to respond effectively in the event of another major disease outbreak, and although some response measures, such as work-from-home practices, have remained within many organizations' operations, the possibility of future disruption to operations due to health security remains.

- Following the protocols implemented during the COVID-19 pandemic, many organizations have sustained some operational practices to streamline their ability to continue to operate in the event of disruption, including those caused by health concerns.
- The impacts of previous large-scale health incidents, such as pandemics, significantly impacted global supply chains, causing operational disruption and increased costs for businesses across all sectors globally. Although governments and regional authorities have taken steps to improve resilience to such events, their unpredictable nature and vast possible geographical spread indicate that future events remain likely to have similar-level impacts.
- The likelihood of country / region-specific disease outbreaks in 2025 remains a pertinent issue for businesses with local and international operations, and although a pandemic-like health security event in this timeframe is unlikely, responses to localized disease outbreaks are likely to indicate potential widescale implications of future high-impact health events.

Scenario	Scenario condition	Assessed likelihood
Infectious disease outbreaks decline in frequency and intensity globally, with effective vaccines for high-impact diseases developed and utilized on mass in worst affected areas.	Improves	Unlikely (25%)
Localized disease outbreaks are met with largely effective government / authority responses, limiting significant health and business operations impacts, however, less developed regions continue to face moderate health security concerns.	Baseline	Likely / Probable (60%)
A large-scale global health security event causes significant disruptions, including via lockdowns, impacting business and supply chain operations.	Worsens	Highly unlikely (15%)

- ✓ Maintain awareness of viral infections that are likely to spread and ensure that workers in office-based roles can work from home to reduce infection transmission among employees.
- ✓ Consider creating business operation guidelines in a pandemic circumstance to ensure a smooth transition of procedures and maintain minimal impact on the organization's business as usual, including across supply chains.
- ✓ Monitor minor disruptions to supply chains affecting organizations to identify patterns and possible escalations.
- ✓ Implement heightened sanitary procedures at workplaces to reduce transmission of infectious diseases.

Indicators

- Corporate organizations request employees with office-based roles to work from home and reduce attendance in the office.
- Surveillance and monitoring of the general public visiting / attending closed public spaces where transmissions are highly likely to occur.
- Increased call for front-line workers such as nurses and doctors to treat patients likely infected by infectious diseases.
- Increased funding from the Government for vaccine campaigns and vaccine manufacturing organizations.

Implications

- Reduced workforce in affected regions / countries causing disruptions to business as usual.
- Shortage in materials for products due to lack of funding and attention given to supply chains amid concerns over the spread of infections.
- Possible travel restrictions to affected areas disrupting international business operations.
- Reduced funding from the Government due to increased attention and finance capabilities provided to assist vaccine campaigns.
- Increased presence of conspiracy theories and information disorder surrounding disease outbreaks is likely to be observed on social media, heightening the threat of unrest.

Securitas

03

Regional Security - AMEA

2024 Significant Activities - AMEA

JANUARY

A 7.6 magnitude earthquake in Japan resulted in ~238 people killed and ~1,300 injured, causing significant public services and supply chain disruptions on 1 January.

FEBRUARY

A lone gunman, also armed with a suicide vest, took seven employees hostage after infiltrating a Proctor & Gamble plant in Gebze, Türkiye, on 1 February. His motive was to stimulate an end to the Gaza-Israel conflict and to incite the Egyptian and Israeli Governments into opening the Rafah border crossing so humanitarian aid could enter Gaza.

MARCH

Hundreds of protestors took to the streets of New Delhi for several days, with dozens of opposition protesters arrested as they tried to march to Prime Minister Narendra Modi's residence on 26 March after a major opponent of the PM was arrested on 22 March following accusations of corruption.

APRIL

In retaliation to Israel's attack on Iran's consulate in Damascus, Syria, on 1 April, Iran and its proxy groups in the Middle East launched ~300 drones and missiles at Israel on 13 April. 99% of the missiles and drones were intercepted by Israel and foreign nations with assets in the region, such as the UK and the US.

MAY

US President Joe Biden announced a range of new tariffs aimed at Chinese electric vehicles, semiconductors, and solar equipment on 14 May. The announcement targeted strategic sectors, maintaining some existing tariffs by the Trump administration and significantly increasing some tariffs on other sectors deemed critical to national security.

JUNE

The Yemeni Houthi movement claimed it conducted four coordinated attacks with Islamic Resistance in Iraq targeting ships in Israel's Haifa port throughout June. The Houthis expanded their military capabilities by utilizing newly built missile technology and reportedly launched 'Hatem 2' hypersonic missiles at the Liberian-flagged container ship MSC Sarah V in the Arabian Sea.

JULY

Bangladeshi students began protesting after the High Court reinstated a law requiring 30% of highly valued and well-paid civil service jobs to be reserved for the descendants of freedom fighters. Clashes between police and protestors resulted in ~150 deaths and ~2,500 arrests, after which the army was called in to enforce a curfew on 20 July with soldiers receiving a 'shoot-at-sight' order.

AUGUST

The Australian Security Intelligence Organization (ASIO) raised the country's terrorism threat level from 'possible' to 'probable' on 5 August. The decision came after the ASIO reported that it had disrupted or responded to eight terror incidents since April 2024 including the Wakely church attack in Western Sydney.

SEPTEMBER

Cross-border conflict between Israel and Hezbollah escalated significantly, raising regional tensions and prompting Israel to launch a ground incursion into southern Lebanon. Lebanese Armed Forces withdrew 5km from their border positions ahead of the operation to minimize confrontation with the IDF

OCTOBER

Five people were killed and 22 injured in a terror attack at Turkish Aerospace Industries (TUSAŞ) headquarters near Ankara, Türkiye involving two gunmen from the Kurdistan Workers Party (PKK). TUSAŞ manufactures drones and other ordinances used by the Turkish Airforce against PKK members in northern Iraq and Operation Euphrates Shield in Syria, which is believed to be the reason its headquarters was chosen as the attack target.

NOVEMBER

Syrian rebel forces, led by Islamist militant group Hayat Tahrir al-Sham, launched a major offensive on 27 November that reached the center of Syria's largest city, Aleppo city, by 29 November, marking their first significant territorial advance since being forced out in 2016. The rebels advanced, capturing ~40 towns and villages in northern Aleppo province, with commanders attributing their rapid progress to reduced Iran-backed forces in the region. The offensive has resulted in at least 260 casualties, including dozens of civilians.

DECEMBER

South Korea's Parliament successfully impeached President Yoon Suk Yeol in a second vote on 14 December, following controversy over his declaration of martial law earlier in the month, with tens of thousands of demonstrators gathering in Seoul in celebration. The parliament also voted to impeach acting President Han Duck-soo, after the opposition Democratic Party submitted a motion to impeach Han due to his reluctance to formally appoint three nominated justices to the Constitutional Court ahead of its review of insurrection charges against impeached President Yoon.

Changing Middle East security landscape as Iranian regional doctrine fractured

Threat actors continued to exploit Middle East tensions in 2024, but the Iranian-led Axis of Resistance (AOR) has been disrupted by Israeli and allied efforts and most recently fractured by the fall of the AOR's division in Syria: Bashar al-Assad's regime. Iran is reeling from significant blows to the AOR, particularly as Bashar's Syria was a primary host for Iran to supply proxy militant groups in Lebanon, Iraq, and elsewhere. Iran will likely pursue other forms of deterrence against Israel and the US, including increased aggressive posture and signaling around Iran's nuclear capabilities and reevaluating its AOR-reliant defense, shifting the regional security landscape.

- The ongoing Israel-Hamas and Israel-Hezbollah conflicts have evolved into a broader regional confrontation marked by unprecedented direct military exchanges between Iran and Israel, representing a significant escalation beyond the traditional proxy warfare dynamic. This is likely to continue and increase throughout 2025 as Iran repositions itself and reinforces the AOR.
- The election of US President-elect Donald Trump introduces renewed strategic calculations, particularly given his previous *"maximum pressure"* approach to Iran and strong support for Israel. While direct conflict between Iran and the US remains unlikely, increased US pressure and the degradation of the AOR will likely back Iran into a 'corner' that risks greater escalation.
- Strong US support for Israel in the Gaza conflict will likely create opportunities for Iranian proxies in Iraq and Syria to expand their influence. This dynamic, coupled with ongoing discussions of US / coalition withdrawal from Iraq by September 2025, presents potential opportunities for Iran to attempt to reinforce its AOR in the Middle East, raising new potential threat actors.

Scenario	Scenario condition	Assessed likelihood
Aggressive US posturing towards Iran through increased sanctions, threats of conflict, and Iran's fractured AOR leads to de-escalation and reduced Iranian proxy attacks due to fear of wider direct conflict.	Improves	Highly unlikely (10%)
A more aggressive US posture under Trump towards Iran and its proxies escalates tensions, with continuing attacks on US interests by fractured AOR proxies while Iran recalculates and likely escalates nuclear posturing, alongside reciprocal US attacks on Iranian interests.	Baseline	Likely (70%)
Tensions escalate, and a flashpoint leads to direct Iran-US conflict, leading to regional conflict, and a material escalation of Iran's nuclear capabilities / threats.	Worsens	Unlikely (20%)

ADVISORY

- ✓ 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.
- ✓ Review and enhance cyber security measures to protect against state-sponsored attacks, particularly focusing on critical infrastructure and sensitive data.
- ✓ Maintain awareness of the potential for Middle East tensions to continue to motivate threat actors internationally, including activists and terrorists / extremists.

Indicators

- Changes in frequency and sophistication of AOR attacks on US interests across the Middle East, particularly in Iraq and Syria.
- Rising incidents of maritime security threats in the Red Sea and Persian Gulf, particularly targeting vessels linked to Israel or Western interests.
- Growth in anti-Western rhetoric and recruitment activities by Iranian-backed groups, especially in areas with reduced US presence.
- Shifts in US troop movements and resourcing to implement renewed pressure on Iran.

Implications

- Rapid shifts in regional dynamics following the January 2025 US transition of power, providing an unpredictable business landscape.
- Shift in Iranian regional doctrine as the AOR is disrupted and fractured to new deterrents.
- Continued disruption to regional supply chains and shipping routes, particularly affecting energy, and maritime sectors.
- Strategic shift required in business operations as US military withdrawal creates new security dynamics, particularly in Iraq and Syria.
- Western organizations face increased hostility and possible targeting in areas with strong support for Palestine / Iran.

China’s persistent targeting of international businesses with legislation and scrutiny

China increased scrutiny and legislative targeting of international organizations throughout 2024, largely in response to alleged threats to Chinese interests, including national security, markets, and state and corporate espionage. Organizations in the defense, technology, manufacturing, and finance, industries are typically targeted, however, wider laws and policies often cause barriers to market entry and threaten business operations across sectors.

- The Government's widening of national security, espionage, and data laws, including regarding ‘state secrets’ has caused operational and compliance challenges for businesses with ambiguous interpretations and arbitrary enforcement of laws.
- China has continued to scrutinize organizations’ sharing and handling of data and it is not uncommon for the Chinese state to seek access to businesses’ information and data, which is expected to persist alongside complex geopolitical tensions, and cause physical / legal disruption to businesses operating in the country.
- Direct disruptions to international businesses also include police raids, corporate legal action, and employee arrests, with China’s sensitivity to national interests and market threats causing businesses considerable uncertainty and compliance issues within their Chinese operations, particularly around ambiguous covenants such as ‘state secrets.’

Scenario	Scenario condition	Assessed likelihood
China's desire to maintain its business reputation outweighs its scrutiny of foreign organizations, making the business environment easier.	Improves	Highly unlikely (10%)
China continues to enforce national / security interests arbitrarily to crack down on organizations / individuals deemed to be in breach of Chinese law and interests.	Baseline	Likely / Probable (55%)
Chinese security laws are extended to international organizations’ regular business practices. BAU activities are classed as espionage / threats, leading Chinese authorities to carry out high-profile arrests, posing serious threat to business operations.	Worsens	Unlikely (35%)

- ✓ Maintain awareness of Chinese legislative policies and establish lines of communication with the legal teams. Legal teams should be briefed and regularly consulted on fast-moving Chinese legislation to avoid legal challenges.
- ✓ Be prepared to change business practices to conform to legal issues. Ensure employees are aware of new legal requirements and senior employees are aware of the potential for Chinese authorities to open investigations into organizations.
- ✓ Organizations operating in China should have extensive continuity clauses prepared in the event of legal and business issues, to avoid significant impacts to operations and loss of earnings

Indicators

- Increased flashpoints and resultant degradation of China-Western diplomatic and / or trade relations.
- Continued implementation of security laws in Hong Kong, and isolated incidents of foreign nationals / business travelers being arrested in entry / exit from China.
- Chinese investigations and intervention amid private sector disputes, particularly involving Western organizations, persist.
- The Government continues to establish arbitrary, inconsistent and / or expansive business laws with wide interpretations.

Implications

- Potential closure of organizations’ Chinese operations due to legislative and policy action, influenced by decreased investor confidence in the country.
- Pressure on governments to defend organizations operating in China inciting tit-for-tat diplomatic and trade sanctions.
- Organizations, particularly in defense, technology, and auto industries, will be required to invest in measures to offset targeting and disruptive legislation.
- Increased raids on foreign offices, arrests / detention of high-profile VIPs, arbitrary enforcement of ‘national security' interest, disrupting operations and heighten tensions.

Africa faces persistent energy disruptions and food shortages

Energy and food insecurity remain pressing challenges across many African states, frequently disrupting local businesses and diminishing the public's quality of life. Numerous countries in the region face significant obstacles to service delivery due to limited economic resources, often relying heavily on foreign aid to support their economies. A range of factors will likely continue to contribute to these insecurities, including internal issues like climate events, ongoing conflict, and political corruption, as well as external pressures such as conflict in other parts of the world.

- Frequent power outages, driven by outdated and damaged grid infrastructure, are common in states such as Nigeria and South Africa, where routine blackouts disrupt local business operations and will likely continue while these issues persist. Food shortages will likely remain a challenge in regions like the Democratic Republic of Congo and Sudan, often exacerbated by long-term conflicts that destabilize supply chains or regular severe weather events that lead to crop failures causing famines, health crises, and population displacement. As a result, continued mass cross-border migration is probable.
- It is highly likely these ongoing issues will continue to affect African economies and heighten tensions both within and between African nations as local communities and states compete for limited resources and clash over high cross-border migration levels.
- The production of essential exports, including oil and precious minerals will likely suffer as a result, creating supply chain disruptions that extend globally. Continued trade revenue reductions are probable, maintaining a high-risk environment that will likely continue to deter foreign investment in key African industries.

Scenario	Scenario condition	Assessed likelihood
States affected by power shortages upgrade their power grids leading to a decrease in outages, while states receive increased foreign aid that effectively prevents further famines.	Improves	Highly unlikely (10%)
States continue to face power shortages leading to further business disruptions, while food shortages continue to cause famine and influence increasing immigration levels.	Baseline	Likely / Probable (60%)
Further incidents of conflict and severe weather drive a significant increase in energy and food insecurity severely pressuring local economies and foreign relations.	Worsens	Unlikely (30%)

ADVISORY

- ✓ Implement alternative power sources, such as uninterruptible power supplies (UPS), at sites in countries with frequent power shortages to minimize operational disruptions during outages.
- ✓ Closely monitor climate developments and conflict situations to anticipate food shortages that will affect employees and plan response strategies to address their needs effectively.
- ✓ Diversify trade networks to strengthen supply chain resilience and support local economies, fostering a more stable environment for energy and food production.

Indicators

- Governments announce power cuts or resource shortages at energy-producing plants.
- An increase in fuel and energy costs influenced by limited domestic production or global trade disruptions.
- Heightened political and social unrest protesting the cost of living and resource access.
- An increase in migration and population displacement into neighboring states.

Implications

- Potential operational disruptions resulting from blackouts and increased costs due to heightened reliance on alternative sources of electricity.
- Labor instability and increased labor costs as skilled workers migrate to avoid economic insecurity.
- Brand and reputational damage as businesses are perceived as failing to contribute to local relief operations or protect their employees from humanitarian crises.
- Conflict and political unrest over resource scarcity deters investment and undermines investor confidence in businesses active in the area.

The rise of self-initiated threat actors in Asia

Increased digitization and automatization of countless aspects of society are likely to continue enabling self-initiated threat actors within Asia to remain an elevated threat in 2025, fueled largely by increased societal polarization. Self-initiated threat actors in Asia can take many forms but the most prominent in 2024, and likely to remain so in 2025, is disenfranchised young males engaging in 'self-initiated' style attacks in China, Japan, and South Korea. These threat actors typically engage in broad-spectrum targeting of the public, primarily women and foreigners, but are also known for specific attacks on political figures and organizations, with online forums and social media also playing a key role in the motivation of self-initiated threat actors.

- As indicated in self-initiated attacks in 2024, perpetrators tended to utilize commonly accessible instruments to cause harm, including bladed weapons, although vehicles and chemical accelerants are also common weapons. Attacks are highly visible and usually occur in busy public areas, maximizing potential damage and public distress.
- These tactics will highly likely continue to be employed by individuals due to their ease of being obtained and the ability to maintain surprise against their target, law enforcement, and the media. In remote instances, improvised weapons such as pipe bombs and ad hoc firearms are utilized, but these instruments are commonly reserved for specific targets such as politicians.
- The rapid unregulated development of 3D printers and the rise of 3D-printed firearms are unlikely to increase in prominence due to countries' stringent ammunition controls, further enhancing self-initiated threat actors' capabilities to undertake attacks while evading detection by authorities.

Scenario	Scenario condition	Assessed likelihood
New regulations are introduced across multiple countries empowering law enforcement to access online information of suspects to determine the validity of threat actors, allowing them to effectively detect and deter attacks.	Improves	Highly unlikely (20%)
Self-initiated threat actors continue to target specific and broad-spectrum targets, employing tactics consistent with previous years, with attacks steadily increasing in frequency and impact.	Baseline	Likely / Probable (55%)
Threat actors escalate tactics by employing more sophisticated ad hoc weapons resulting in a higher volume of mass casualty events undetectable by authorities.	Worsens	Unlikely (25%)

- ✓ Organizations should assess their potential exposure to self-initiated threat actors due to their corporate identity, their industry, or their business partners / customers / suppliers.
- ✓ Raise awareness among employees of potential threats associated with self-initiated actors, and practical guidance for staying safe and secure.
- ✓ Ensure security personnel are trained in recognizing hostile reconnaissance from external and internal threat actors.

Indicators

- Increased activity on internet message boards and alternative social media commonly used by individuals disenfranchised with wider society, including possible mentioning of intentions or a manifesto.
- Perpetrators conducting hostile reconnaissance of the intended target to formulate a plan of action and possible countermeasures effectively.
- Increased use of varied tactics by self-initiated threat actors aiming to heighten the impact of attacks.
- Targeting of organizations associated with current events in extremist propaganda.

Implications

- Mass casualty events posing significant threats to life, including organizations' employees, as well as businesses' people, property, and assets in vicinity of attacks.
- Heightened threat sensitivity to real and potential terror incidents resulting in increased security, impacting business operations, particularly for organizations operating internationally.
- Organizations required to increase spending on protection measures for employees, including executives, as well as during travel.
- Organizations perceived to facilitate attacks, including technology organizations, face legal repercussions.

04

Regional Security - Americas

2024 Significant Activities - Americas

JANUARY

Ecuadorian President Daniel Noboa declared a 60-day state of emergency on 8 January in response to acts of violence and unrest after a leader of a drug cartel escaped prison on 7 January. The state of emergency allowed authorities to suspend the rights of citizens, send the military into prisons, and impose a nightly curfew.

FEBRUARY

Record-breaking rainfall in California resulted in flash flooding, mudslides, and power outages throughout the first week of February. The rainfall prompted the Governor to declare a state of emergency in eight counties and officials issued evacuation orders for some neighborhoods in the south of the state.

MARCH

A major bridge collapsed at the US Port of Baltimore after being struck by a cargo ship on 26 March resulting in all marine traffic being suspended until further notice, and six workers missing, presumed dead. The collapse blocked most shipping to and from the Port of Baltimore for 11 weeks.

APRIL

A coordinated economic blockade organized by the US-based activist group A15 Action, in solidarity with Palestine, targeted multiple cities across North America on 15 April. The group self-proclaimed itself as an independent actor; however, multiple established pro-Palestine activist groups joined the action call to disrupt logistic hubs and curb the flow of capital worldwide.

MAY

~580,000 people were displaced and ~2.3 million people were impacted by the torrential rain and floods that have afflicted the Rio Grande do Sul state in Brazil throughout May. Authorities estimated that the situation would take months or even years to return to normal, with 90% of the state's 497 municipalities impacted, with 418 declaring a state of emergency or disaster.

JUNE

A failed military coup occurred in La Paz on 26 June as General Juan Jose Zúñiga attempted to remove President Luis Arce from power. Military personnel and armored vehicles took up formations in Plaza Murillo. General Zúñiga stated that the attempted coup was orchestrated by the President to boost his popularity with the electorate.

JULY

Former President Donald Trump was subject to an assassination attempt during a campaign rally in Butler, Pennsylvania, on 13 July. The attempt resulted in two casualties and one fatality before the shooter, Thomas Crooks, was neutralized by the US Secret Service sniper team.

AUGUST

Strikes across two of Canada's main railways, Canadian Pacific Kansas City and Canadian National Railway threatened major disruption to businesses and supply chains on 22 August. The two main freight rail organizations locked out ~10,000 unionized workers when negotiations over a new labor contract reached the deadline without an agreement.

SEPTEMBER

Severe droughts and multiple cases of human activity caused significant wildfires to spread across several South American states, with Bolivia and Peru declaring national emergencies on 7 September and 18 September.

OCTOBER

Hurricane Milton, which made landfall along Florida's West Coast, was the second most intense Atlantic hurricane ever recorded in the Gulf of Mexico and brought sustained wind speeds of up to 148 km/h and over 330 mm of rainfall in specific areas. Milton caused significant disruption, killing ~32 people and inciting ~$85 billion in damages, while commodity shortages and disruption to transportation services persisted in the days following the event.

NOVEMBER

Republican candidate and former President Donald Trump won the US presidential election, defeating his Democratic opponent Kamala Harris on 6 November. Election Day occurred against the backdrop of a heightened threat environment, with multiple bomb threats sent via mail to polling locations in several states, with many purportedly originating from "Russian domains." The FBI warned that its name and brand were being used in disinformation to promote false election-related narratives.

DECEMBER

The CEO of the largest US private healthcare provider UnitedHealthcare, Brian Thompson, was fatally shot on 4 December outside the Hilton Hotel in New York City. Authorities initially arrested the suspect, Luigi Mangione, on firearms charges but he was later charged with murder after being arrested with a silencer and gun that were consistent with the weapon used. Since Thompson's murder, there has been an increase in threats targeting healthcare and insurance companies, primarily malicious communications intended to intimidate and harass. The increase in threats prompted US companies to enhance security measures for their executives.

US election result influences political partisanship

The US political landscape is becoming increasingly polarized as explicit socio-economic factors, underlying divisions, and geopolitical inputs, stimulate partisan political views that politicians, businesses, media, and malicious threat actors are further exploiting. Resultingly, discord between members and supporters of opposing political parties is manifesting through increasingly hostile views, commentary, and actions. This discontent has also recently been linked to violent and terror-related incidents across the US, with this threat expected to become increasingly prevalent throughout 2025 as the Trump administration comes into office.

- Poignant voter issues such as abortion rights, gun laws, and immigration policy are at the forefront of the political divide in the US and act as key drivers of individuals' political stances. They also have the potential to impact business operations directly and indirectly, with certain organizations being targeted by threat actors due to their association with these issues.
- The volatile and unpredictable political climate surrounding these issues has forced strategic operational changes relating to facets such as hiring policy, business partnerships, and commercial image. Those at the more extreme ends of the political spectrum are garnering increased support and bringing their views further into the mainstream consciousness, simultaneously, political violence and harmful rhetoric are intensifying.
- Political events, such as elections, are acting as flashpoints for increased political violence that is worsened or partly instigated by information disorder, with political activists increasingly targeting assets belonging to opposing political groups / parties and electoral infrastructure, resulting in localized disruption and a heightened security landscape.

Scenario	Scenario condition	Assessed likelihood
Partisan lines degrade and those with opposing views are increasingly united through compromise and policy overlap, resulting in declining political violence and harmful rhetoric.	Improves	Unlikely (25%)
The political landscape remains polarized as elections, protests, and geopolitical events act as flashpoints for escalation. Information disorder continues to contribute to polarization.	Baseline	Likely / Probable (70%)
Significant partisanship reaches a climax and manifests through legislative breakdown, widespread political violence, and the direct targeting of figureheads, certain societal groups, and businesses.	Worsens	Remote (5%)

- ✓ Organizations are advised to maintain awareness of the political calendar and the potential for unrest to occur as a result.
- ✓ Businesses should consider reviewing their portfolios to identify any elements that could be perceived as being connected to a political party / group and could be targeted during increased unrest.
- ✓ Organizations are advised to maintain an understanding of information disorder and the information landscape, especially regarding information on contentious issues, and ensure employees are educated on potential impacts.

Indicators

- The stance of political parties on key issues is generally in opposition resulting in less bipartisan legislation passing.
- Activist actions related to divisive issues force operational changes for businesses in all sectors.
- Isolated incidents of political violence occur alongside political flashpoints.
- Information disorder contributing to political violence and partisan views is identifiable.
- Those on the extremes of the political spectrum are active and widespread in the political space, especially online.

Implications

- Organizations will likely experience security threats related to political violence and unrest
- Employee morale within certain organizations will likely become further politicized and, in some cases, hostile.
- Organizations with connections to political parties / figureheads will likely be targeted.
- Links between certain domestic and foreign businesses will likely degrade due to political destabilization and insecurity.
- Possible violent or terror / extremist incidents fueled by the domestic political landscape result in mass casualty events impacting security in effected states and country-wide.

Climate change-induced drought in South American waterways

Climate change, largely driven by global warming, continues to pose a significant threat to the environment and resource security globally, with its impacts being experienced in regions of the Global South that are heavily reliant on using the natural environment to drive business and industrial operations, and are therefore more vulnerable to climate change motivated threats, such as drought.

- Waterways across South America, including canals and rivers, are intrinsic to business operations, supply chains, energy production, agriculture at all scales, and overall, the lives of millions of people who depend on them for mobility, resources, and income, with specific waterways integral to international trade.
- Drought puts these socio-economic elements at risk by reducing the discharge and volume of waterways to the point where they become inoperable by most vessels and redundant in the case of energy production, increasing costs for businesses that rely on their services. Resource competition can be instigated, leading to food and water shortages and threats to human health.
- Governments across South America have for many years implemented legislation and invested in projects designed to protect waterways from drought, however, due to global warming continuing largely uninterrupted, the frequency and severity of droughts are increasing, rendering current government efforts obsolete in most cases.
- As businesses become more reliant on operations in the region, the need for comprehensive regulations to limit long-term impacts is likely, with organizations likely to face increasing scrutiny over their environmental, social, and governance policies.

Scenario	Scenario condition	Assessed likelihood
Climate change is successfully tackled and the frequency and severity of drought in South America declines, enabling government projects to better protect waterways.	Improves	Remote (5%)
Severe drought periods continue to impact waterways causing resource competition, mitigation of trade, and economic damage that extends to organizations internationally.	Baseline	Highly unlikely (20%)
Climate change worsens and drought periods increase in length and frequency, causing irreparable damage to waterways, driving long-term economic damage and water insecurity.	Worsens	Likely / Probable (75%)

- ✓ Organizations are advised to be aware of the impacts of drought and devise risk management plans designed to lessen drought periods' operational impacts.
- ✓ It is recommended organizations evaluate their operations as well as supply chains to reduce their water dependence and drought vulnerability.
- ✓ Organizations should consider investing in studies aiming to improve understanding of droughts business impacts.

Indicators

- Private and government meteorological services warn of impending drought.
- Waterway levels lower during periods of low to no rainfall.
- Water consumption increases due to growing industrial, business, and societal demands.
- Governments invest money into projects designed to alleviate the impacts of drought in the long term, such as reservoirs.
- Increased reports of shipping delays and supply chain disruption due to inoperable waterways.

Implications

- Organizations in South America will likely face operational disruption due to water and energy shortages.
- Organizations will likely experience operational disruption due to supply chain delays and increased costs due to delays and rerouting.
- Internation organizations will likely be negatively impacted by supply chain delays when key waterways are affected by drought.
- Relocation of some business operations in South America becomes increasingly likely so they are not as impacted by drought, inflicting operational disruption, and increased financial challenges.

Proxy tensions endure between the West and China / India

Strategic competition between China and Western powers intensified throughout 2024, marked by increasingly aggressive Chinese military posturing around Taiwan, escalating maritime disputes in the South China Sea, and Chinese state-backed cyber operations targeting critical infrastructure across Canada and the US. These developments have occurred against a backdrop of deepening technological competition and economic rivalry between the world's two largest powers.

- While US-India strategic cooperation is likely to strengthen under Trump's second term, given the leaders' personal relationship and shared focus on countering China, Canada-India diplomatic relations remain severely strained following the Indian-linked assassination of Sikh activist Hardeep Nijjar and the associated diplomatic fallout.
- While direct China-US conflict remains highly unlikely, proxy competition is expected to intensify through cyber operations, influence campaigns, and economic measures. Trump's promised implementation of 60% tariffs on Chinese goods will likely trigger significant economic retaliation from China, accelerating economic decoupling between the two countries.
- Tensions over Taiwan and the South China Sea are likely to intensify, with increased military posturing from both sides, impacting regional security and political / diplomatic relations between affected countries.
- Organizations operating across Asia and North America will likely face growing pressure to navigate these geopolitical tensions while managing supply chain disruptions and market access challenges.

Scenario	Scenario condition	Assessed likelihood
China and the US reach limited trade accommodations while maintaining strategic competition, reducing risks of economic decoupling.	Improves	Unlikely (25%)
Implementation of new US tariffs leads to Chinese retaliation and accelerated economic decoupling, while cyber operations and military posturing increase.	Baseline	Likely (65%)
Major cyber attacks against critical infrastructure coincide with a military crisis over Taiwan, triggering comprehensive economic decoupling and potential conflict.	Worsens	Highly unlikely (10%)

- ✓ Implement comprehensive cyber security measures specifically addressing state-sponsored threats.
- ✓ Develop detailed contingency plans for rapid supply chain reorganization in response to new tariffs.
- ✓ Create flexible supply chain alternatives that can adapt to changing geopolitical dynamics including conflict scenarios.
- ✓ Review and enhance security measures at facilities identified as high-risk for state-sponsored cyber or physical attacks.

Indicators

- Expansion of Volt Typhoon and other state-sponsored cyber campaigns targeting specific sectors (government, energy, transportation, water) across North America.
- Implementation timeline and scope of the Trump administration's proposed 60% tariffs on Chinese goods, and specific Chinese retaliatory measures.
- Increased frequency of Chinese military exercises around Taiwan, particularly those simulating blockade or invasion scenarios.
- Changes in Canadian-Indian diplomatic engagement, particularly regarding extradition requests and intelligence sharing protocols.

Implications

- Organizations involved in critical infrastructure or sensitive industries will likely face increased threats from state-backed cyber threat actors.
- Major disruptions to global supply chains and increased operational costs due to China-US tariff escalation and economic decoupling.
- Increased compliance complexity for multinational corporations operating across Chinese and Western jurisdictions.
- Growing pressure on businesses to ‘choose sides’ in US-China technology competition, with legal and regulatory backlash expected for ‘non-compliant’ organizations.

Latin American threat actors’ expansion into extractive industries

Organized Crime Groups (OCGs) have consistently posed threats to extractive industries, including oil and gas and mining, across Latin America, with this expected to continue throughout the region in 2025, largely targeting small to medium-scale organizations that are domestically operated. Attacks have posed threats to organizations' operations, including the safety of employees at targeted sites, as well as further contributing to domestic and regional instability, fueling criminal activities.

- The oil and gas and mining industries enable OCGs to diversify their financial streams into what appears to be a legal business, while allowing illicitly gained finances to be money laundered for personal or organizational use. OCG utilization of corruption of authorities to conceal or enable their illicit operations is also commonly observed, making this trend increasingly complex to combat for organizations' impacts.
- Government responses to threats are unlikely to improve, as countries such as Peru and Bolivia face significant domestic unrest over issues unrelated to mining operations, while Ecuador faces an ongoing energy crisis that is unlikely to be resolved in the near term. Recent Colombian violence and breakdowns of ceasefire agreements with armed guerilla groups indicate renewed kinetic action in the near term, further impacting the extractive industries.
- Environmental activist groups and Indigenous populations are also likely to act as threat actors in an increasing capacity in 2025, with motives to shut down mining and oil and gas operations likely through nonviolent protests at sites. Although large-scale international organizations are likely to continue to be protested, the inability to have immediate / lasting impacts is unlikely to make them appealing targets compared to domestic operations.

Scenario	Scenario condition	Assessed likelihood
Governments increase response to threat actors' interference in extraction operations, more effective legislation, and police operations.	Improves	Highly unlikely (15%)
Threat actors continue to prioritize the targeting of domestically operated extraction organizations, with attacks resulting in operational disruption and increasing threats to life for employees.	Baseline	Likely / Probable (60%)
Internationally operated extraction organizations face increased targeting by threat actors, causing long-term operational disruption, and impacting investor confidence in the region.	Worsens	Unlikely (25%)

- ✓ Develop robust threat assessment protocols for identifying and managing credible threats to the organization, which integrate with security protocols for people (including Executives), property, operations, and brand and reputation.
- ✓ Implementing protocols such as anti-money laundering frameworks will allow organizations to raise their employees’ awareness of money laundering tactics and prevent potential exploitation by OCGs.
- ✓ Assess supply chain vulnerabilities that could be exploited by threat actor targeting of the Latin American extraction industries.

Indicators

- Increased shows of force and / or aggression by OCGs both in existing states and new areas.
- Targeting of mining and extracting sites as OCGs seek to expand their revenue streams and establish control.
- Tensions and clashes in resource-rich areas between locals, governments, OCGs, activist groups, and extractors (legal and illegal).
- Increased or more severe seasonal weather conditions triggering more frequent or heightened environmental / indigenous activism.
- National crises develop preventing effective Government response to threat actors.

Implications

- Domestic extraction organizations will likely incur increased costs for security to counter threat actor interference.
- Increased access to revenue by threat actors is likely to result in the intensification of violence and power of OCGs and paramilitaries.
- International extraction organizations are unlikely to expand operations in the region if threat actors pose an increased risk to revenue and employee safety.
- Decreased investor confidence in the sector / region will likely negatively impact domestic economies, further driving OCG activity and regional instability.

Securitas

05

Regional Security - Europe

2024 Significant Activities - Europe

JANUARY

French farmers protested throughout January, including blocking highways and dumping crates of imported produce, in protest of funding cuts and policies. The authorities reported that ~15,000 police were mobilized to prevent tractors from entering Paris and other cities on 30 January, as farming unions called the actions a ‘siege’ on the capital.

FEBRUARY

The Russia-Ukraine conflict marked its second anniversary, with leaders from various Western nations visiting Kyiv to mark the anniversary and reaffirm their support for Ukraine. Russian authorities announced the death of Russian opposition leader, and prominent Putin critic, Alexei Navalny, sparking protests globally and resulting in 400~ arrests at memorials across Russia.

MARCH

~139 people were killed, and ~182 injured during a terrorist attack carried out by four armed suspects carrying automatic weapons at the Crocus City Hall concert venue in Moscow, Russia, which was claimed by the Islamic State Khorasan. Russian President Vladimir Putin stated the attackers were trying to flee to Ukraine and vowed to investigate Western involvement.

APRIL

Online channels linked to the Islamic State reshared previously made calls for terror attacks targeting sporting events in Europe. The calls specified stadiums in London, Madrid, and Paris as targets for attacks, with the venues hosting significant European Champions League football matches. All matches went ahead without reported incidents.

MAY

Slovakian Prime Minister, Robert Fico, was shot in the abdomen on 15 May by a 71-year-old as he was leaving a meeting of political supporters at a cultural center in the town of Handlova, Slovakia. The attack was reportedly politically motivated.

JUNE

One person was killed and two were injured after a knifeman targeted a EURO 2024 watching party in Magdeburg on 15 June, while an axe-wielding man threatened fans at a EURO 2024 fan zone and was shot dead by the police in Hamburg on 16 June.

JULY

Climate activist groups Just Stop Oil and Last Generation demonstrated at airports throughout Europe, in support of ‘Oil Kills’, an international activist campaign *“to end oil, gas, and coal by 2030”*. The actions involved members of the groups gluing themselves to runways, conducting sit-ins, blocking roads, and walkways, and displaying banners highlighting climate crisis issues.

AUGUST

Three people were killed and eight injured in a knife attack at a cultural festival carried out by a Syrian man with purported links to Islamic State (IS) in Solingen, Germany. Police detained the attacker, identified as Issa Al H on 24 August with IS claiming that they were a ‘soldier’ of IS and that their actions had been carried out in ‘revenge’ for Muslims in Palestine and worldwide.

SEPTEMBER

Storm Boris caused significant damage and disruption across Central and Eastern Europe throughout September. Flooding, driven by high rainfall, caused ~23 deaths across Austria, Italy, Poland, and Romania and damaged thousands of homes across the region. Heavy rainfall in Czechia caused ~15,000 to be evacuated from the Moravia-Silesian region, with Poland also declaring a ‘state of natural disaster’.

OCTOBER

Georgia held parliamentary elections with the ruling, pro-Russia, Georgian Dream party declaring victory after allegedly winning ~53% of the vote. Opposition parties refused to accept the results, with allegations of widespread electoral violations, including ballot stuffing and voter intimidation, while the biggest opposition party, United National Movement, claimed its headquarters came under attack on election day.

NOVEMBER

Two subsea fiber-optic communication cables in the Baltic Sea linking Finland, Germany, Lithuania, and Sweden were damaged by a Chinese cargo ship purportedly captained by a Russian national on 17 November, increasing concerns of state-backed sabotage targeting undersea infrastructure in the region. Damages resulted in significant communications disruption, with signals rerouted through alternative Baltic Sea cables.

DECEMBER

Five people were killed and ~200 injured after a vehicle was used to attack crowds at a Christmas market in the city of Magdeburg, Germany, on 20 December. Authorities reported that the car drove into the market at high speeds after it had gained access to the area via an emergency exit route. The suspect was immediately arrested by police at the scene and identified as 50-year-old Saudi Arabian psychiatrist Taleb Al-Abdulmohsen. Authorities believe that the attack was self-initiated, with no link to known threat actors identified.

Russia escalates sabotage campaign across Europe

Russia continues to conduct espionage and sabotage actions across Europe as part of a coordinated gray zone warfare (GZW) campaign targeting critical infrastructure and organizations engaged in commercial relations with Ukraine. Further sabotage actions are highly likely to persist as inter-state tensions continue to rise regarding Western support for Ukraine. GZW is used to thwart, destabilize, weaken, or gradually attack adversaries, allowing the perpetrator to remain anonymous or deny responsibility using conventional and unconventional means and proxies.

- Russian GZW operations have historically targeted aerospace / defense facilities, critical national infrastructure (CNI), financial services, public services, and transport / logistics organizations, especially those linked to Ukraine using physical and cyber tactics, techniques, and procedures (TTPs). Incidents have primarily been observed in Central and Eastern Europe, Scandinavia, and the UK.
- Mass casualty events remain unlikely due to the threat of retaliatory action from Western actors, localized casualties caused by Russian sabotage actions are possible, while further damages to undersea infrastructure, CNI, and aerospace and defense organizations' assets remain highly likely.
- Sabotage or attacks on CNI have the potential to cause country and sector-wide impacts, including operational disruptions and supply chain delays, with the increasing sophistication of tactics used and frequency of attacks posing a rapidly growing threat.

Scenario	Scenario condition	Assessed likelihood
Western states place further restrictions on Ukrainian long-range weapons use against Russian military targets, reducing the likelihood of sabotage actions by Russian-affiliated threat actors.	Improves	Highly unlikely (10%)
Ukraine uses Western long-range conventional weapons to attack Russian military assets, increasing tensions and the likelihood of sabotage actions damaging infrastructure and the private sector.	Baseline	Realistic / Possible (40%)
Tensions escalate causing threat actors to utilize more extreme TTPs, increasing the likelihood of casualties and damages to corporate assets.	Worsens	Realistic / Possible (50%)

- ✓ Organizations commonly previously targeted sectors are advised to maintain an enhanced security posture and take adequate provisions to mitigate the risk of damages to assets and personnel.
- ✓ Maintain contact with authorities and follow advice on preventative measures to safeguard assets and facilities.
- ✓ Increase patrolling and monitoring of vulnerable business areas which will possibly be exploited by threat actors.
- ✓ Assess potential supply chain impacts caused by damage / disruption of CNI or specific sector essential for business operations.

Indicators

- Increasing reports of suspected Russian sabotage as observed across Europe – from public and private sectors – including those associated with other nation-state-back threat actors (China, Iran, North Korea).
- Increased targeting of Russian military assets using Western-supplied weapons.
- Russian authorities maintaining plausible deniability of actions.
- Rising exploitation on insider threats, including within supply chains, to heightened impacts of sabotage attempts.

Implications

- Heightened cyber and physical threats, increasing the risk of asset damages and prolonged operational disruptions within the public and private sectors.
- Increasing hostile tactics are likely to pose a heightened risk of civilian casualties.
- Heightened security requirements, and subsequent costs, for at-risk businesses / industries.
- Further restrictions on business relations with Russian organizations, impacting supply chains.
- Possible conflict spread from Ukraine to other European states, significantly impacting regional stability and business operations.

Disruptive and harmful activism proliferates across Europe

Activist groups continued to employ disruptive and harmful tactics, techniques, and procedures (TTPs) in 2024, a trend that will almost certainly evolve in 2025. Environmental activists will likely intensify their use of extreme TTPs to challenge organizations perceived to be contributing to climate change, while anti-war activists will continue to be motivated by global conflicts. Elections and possible gains for far-right political parties will almost certainly embolden far-right activists to conduct more frequent and disruptive actions.

- The targeting of businesses and industries perceived to be linked to activist causes has become increasingly prolific, with ‘successful’ actions highly likely to promote the continuation of high-impact campaigns in the long term. Actions are also likely to include the targeting of supply chains and business relations to maximize the impact of campaigns.
- Some activist groups have been observed to broaden their strategies by engaging in more overt and disruptive actions, leading to harsher legal repercussions and the introduction of new laws that enhance police powers to suppress disruptive protests, even if peaceful, in various countries. This is likely to be further influenced as media coverage and national political discussions increasingly highlight these groups, they will likely escalate the severity of their actions to promote their agenda.
- Activists will continue to develop strategies aimed at maximizing disruption regardless of harsher sentences, including the adoption and modification of tactics between activist groups. The development of more radical TTPs will pose threats to businesses whether they are primary or secondary targets.

Scenario	Scenario condition	Assessed likelihood
Activist actions become less disruptive and damaging, reducing the need for authority intervention.	Improves	Highly unlikely (10%)
Actions continue to receive a significant / immediate response from authorities, leading to arrests of activists, however, legal cases do not progress and are often ruled out / dropped.	Baseline	Likely (55%)
Activists receive significant prison sentences for involvement in actions, leading to backlash from supporters, and activist groups designated as criminal / terrorist organizations causing public unrest.	Worsens	Unlikely (35%)

- ✓ Identify operations, assets, personnel, or partnerships likely to be targeted by activist groups, either directly or by association.
- ✓ Maintain awareness of protests and activism near business assets, and develop response plans to manage scenarios, including enhancing security measures at sites and implementing strategies to minimize operational disruption.
- ✓ Consider developing intelligence monitoring capabilities to identify flashpoints that will likely lead to heightened protest activity.

Indicators

- Any escalations or developments in key global conflicts are likely to act as flashpoints for increased activism.
- Activists continue to be charged with non-violent protest; most cases are likely to be dropped due to perceived legal repercussions, motivating a continuation of activism.
- Disruptive actions as perceived to have a material impact on targeted organizations (i.e. financial or operational difficulties) emboldening groups / individuals to continue campaigns.
- Governments introduce policies regarding restrictions on activism and increase punishments to curtail disruptive and harmful actions.

Implications

- Harsher sanctions and increased restrictive measures on activist groups are likely to embolden them to modify TTPs and increase disruption and damage.
- Degradation of business relations due to activist targeting of supply chains, likely impacting organizations’ operations.
- Reputational damage caused by activist targeting causes increased strained business relations.
- Activist targeting of critical infrastructure poses wider disruption to countries / regions and subsequent business operations.

Europe responds to surge in irregular migration impacting supply chains

Increased irregular migration driven by conflicts, organized criminal group (OCG) activity, and terrorist attacks has caused significant public backlash in Europe, raising concerns over the need for heightened border restrictions which would likely impede logistics operations and supply chains. Notable increases in right-wing rhetoric have been observed, contributing to fragmented government and supranational policy.

- Right-wing / far-right groups will likely demonstrate and exert pressure on European Governments as heightened irregular migration to the bloc will see a probable rise in the immediate to medium term. Ideological clashes with native populations are likely, boosting support for more radical / fringe parties during election periods, indicating increased fragmentation of the EU in the near term, and the imposition of more stringent border measures from liberal states in retaliation.
- OCG activity will almost certainly continue in the immediate term, furthering the likelihood of border restrictions impeding European freight.
- Prospective enhanced restrictions will almost certainly increase delays at land borders across Europe, having tangible economic and operational impacts on organizations dependent on the timely flow of cross-border freight. While direct damage to assets remains unlikely, consumer confidence and reputation loss are possible for organizations impacted by border restrictions imposed in retaliation to irregular migration.

Scenario	Scenario condition	Assessed likelihood
Irregular migration to Europe declines, reducing support for restrictive border policies, and lessening impacts for businesses.	Improves	Highly unlikely (10%)
Irregular migration continues to moderately rise, increasing support for heightened border restrictions, causing delays in a small number of European states.	Baseline	Likely / Probable (55%)
Irregular migration drastically increases, leading to the implementation of stringent land border measures across the EU, influencing significant disruption for businesses and supply chains.	Worsens	Unlikely (35%)

✓ Ensure alternative routing and transport plans are in place to mitigate the commercial risks associated with the possible implementation of heightened border restrictions.

✓ Maintain communication with authorities regarding protest activity and possible implementation of legislation that will alter border arrangements and cause commercial repercussions.

✓ Plan for changes to pricing and availability regarding transport / logistics routes due to likely delays and disruption caused by migration-related issues.

Indicators

- Domestic security issues and conflict influence migration levels in Europe and nearby regions.
- Protest landscape increases in affected European states, with anti-migrant sentiments growing.
- Liberal parties / governments take harsher stances on free movement to appease the electorate.
- Legislation being formally proposed to reduce migration, including references to stricter border security measures.
- Right-wing / far-right groups continue to gain electoral support.

Implications

- Potential disruption to the movement of freight across the region, including fines / penalties for not adhering to heightened regulations.
- Longer time frames on deliveries and potential hold-ups for both consumers and organizations.
- Reputation damage and decline in consumer confidence influenced by service / product delays.
- Financial loss caused by disruption and the fragmented regulatory environment.
- Increased protest landscape causing possible damages to corporate assets.

Persistent multi-sector industrial action amid rising costs

Unionized industrial action will likely continue impacting critical infrastructure operations and the delivery of public services regionwide, leading to potential supply chain interruptions, transport delays for employees, and rising operational costs for organizations. The right to conduct industrial action is guaranteed by the European Convention on Human Rights (ECHR), ensuring that it is unlikely government regulation can be adopted to alleviate the impacts.

- Recent trends in industrial action at the end of 2024 suggest several 'at-risk' sectors, such as healthcare workers striking over working conditions and low wages, organized dock worker's strikes reducing cargo loads in major economic ports, and public transport unions, such as rail industries prolonging strike action.
- Europe is experiencing declines in market shares across multiple industries, highlighted by Germany's automobile industry losing trade to China, and the upcoming Mercosur agreement opening South American agricultural markets to Europe, both likely to produce negative economic impacts domestically and stoke industrial unrest.
- The majority of industrial action will likely be centered on wage disputes and economic conditions, such as inflation and cost of living. It remains probable that economic conditions continue in a downward trend, as the cost of living and inflation increase regionally. Successful cases of union action are likely to motivate workers facing economic challenges in other sectors to conduct industrial action, leading to a likely knock-on effect across different industrial sectors.

Scenario	Scenario condition	Assessed likelihood
Industrial action events decrease as economic conditions improve, leaving fewer impacts on critical infrastructure and public services.	Improves	Highly unlikely (15%)
Economic conditions continue to fall and industrial action consistently involves critical infrastructure and public services, causing subsequent cross-sector disruption.	Baseline	Likely / Probable (60%)
Economic conditions significantly decline, generating organized multi-sector industrial action, and spreading industrial action to new industrial sectors, causing widespread disruption.	Worsens	Unlikely (25%)

- ✓ Organizations should be proactive in monitoring union communications (i.e. websites) and maintain awareness of industrial action trends to stay informed on upcoming industrial action.
- ✓ Organizations with supply chains linked to Europe should develop contingencies such as alternate supply routes to reduce threat exposure during prolonged instances of industrial action.
- ✓ Evaluate exposure threat and consider contingency plans such as working from home in the event of industrial action targeting critical infrastructure, such as transport strikes.

Indicators

- Cost of living and inflation remains high among European nations, leading to wage disputes.
- Successful cases of industrial actions gaining favorable terms for workers, motivating unions and other sectors to partake in industrial action.
- Government regulators continue to mediate ongoing labor disputes with limited success.
- Cost of living and inflation remains high among European nations, leading to wage disputes.
- Successful cases of industrial actions gaining favorable terms for workers, motivating unions and other sectors to partake in industrial action.

Implications

- Disruption of regional supply chains and increased freight costs as alternative routes are used.
- Impacts on deteriorating economic landscape regionally, increasing workers' concerns, as possibility of insider threats resulting from disgruntled employees in extreme cases.
- Rising operational costs for organizations linked with the agricultural sector as strikes increase produce prices.
- Reputational threats to organizations that rely on the timely delivery of goods due to reduced consumer / supplier trust.
- Disruption of regional supply chains and increased freight costs as alternative routes are used.

Securitas

06

Global Security – 2025 Key Dates and Flashpoints

JANUARY

20 January: US Presidential Inauguration.

20-24 January: World Economic Forum in Davos, Switzerland.

22-23 January: The Latam Water Summit will take place in Cartagena, Colombia.

26 January: Belarusian Presidential Election.

27 January: End of 60-day ceasefire between Israel and Hezbollah.

FEBRUARY

9 February: Ecuador General Election.

10-11 February: Third AI Safety Summit hosted by France.

12-13 February: NATO Defense Ministers meeting in Brussels, Belgium.

14-16 February: Munich Security Conference in Germany.

22 February: Third anniversary of Russia-Ukraine conflict.

23 February: German Federal Elections.

28 February – 31 March: Ramadan.

MARCH

5 March: Third Session of the 14th National People's Congress in Beijing, China.

22 March: UN World Water Day.

30 March: Eid al-Fitr.

APRIL

12-20 April: Passover.

20 April: Easter.

21-27 April: IMF and World Bank Spring Meetings in Washington DC, US.

26 April: White House Correspondents Association Dinner, in Washington DC, US.

April-August: The UN World Food Program projects that in this period ~2.3 million people in the Central African Republic will face acute food insecurity without adequate humanitarian assistance.

MAY

1 May: May Day.

1 May: UK Local Elections.

9 May: Russia Victory Day.

12 May: Philippines General Election.

15 May: Nakbah Day.

27 May-1 June: 78th World Health Assembly in Geneva, Switzerland.

May (n.d.): Poland Presidential Election.

JUNE

9-13 June: UN Ocean Conference in Nice, France.

6-10 June: Eid-al Adha.

24-26 June: NATO Summit in The Hague, Netherlands.

June: LGBTQIA+ Pride Month.

June (n.d.): 51st G7 Summit in Alberta, Canada.

JULY

5 – 6 July: Ashura.

31 July: Anniversary of Ismail Haniyeh's assassination.

27 July: Japan's 27th General Election of the House of Councillors.

AUGUST

15 August: India's Independence Day.

17 August: Bolivia General Election.

SEPTEMBER

8 September: Norway Legislative Election.

9-23 September: UN General Assembly New York, US.

September (n.d.): The potential withdrawal of US-led coalition forces from Iraq.

September (n.d.): The Fourth High-level Meeting of the United Nations General Assembly on the Prevention and Control of Noncommunicable Diseases in New York, US.

OCTOBER

1-2 October: Yom Kippur.

6-13 October: Sukkot.

7 October: Second anniversary of the Gaza-Israel conflict escalation.

19 October: IMF and World Bank Annual Meetings in Washington, DC.

20-21 October: Diwali.

NOVEMBER

4 November: Federal legislative elections to fill seats in the US House of Representatives are expected to be held in Florida and New York, and state gubernatorial elections in New Jersey and Virginia.

10-21 November: United Nations Climate Change Conference (COP) 30 will take place in Brazil.

November (n.d.): Chile General Election.

November (n.d.): Ireland Presidential Election.

November (n.d.): South Africa G20 Summit.

DECEMBER

14-22 December: Hanukkah.

25 December: Christmas.

December (n.d.): Central African Republic Presidential election.

Political event
Religious event
Global / national observance
Economic event
Global conflict
Health event
Industry event

Meet the team

Alma Abraham – Junior Protective Intelligence Analyst

Oliver Bacchus – Junior Global Intelligence Analyst

Sophie Cairney – Senior Protective Intelligence Analyst

Matthew Cates – Junior Global Intelligence Analyst

George Chalimourdas – Global Intelligence Team Lead

John Coudriet – Intelligence Analyst (Embedded)

Ermete Del Buono – Junior Protective Intelligence Analyst

Lucy Dickens – Junior Global Intelligence Analyst

Nick Fullick – Global Intelligence Team Lead

Jack Hughes – Junior Global Intelligence Analyst

Alex Johnson – Global Intelligence Team Lead

Sam Kaplin – Global Intelligence Team Lead

Cyan Lynch – Junior Global Intelligence Analyst

Joshua Mendelson – Junior Global Intelligence Analyst

Matthew Phillips – Global Intelligence Team Lead

Max Ross – Junior Global Intelligence Analyst

Nathan Skeet – Junior Global Intelligence Analyst

Tom Wilde – Protective Intelligence Analyst

Brittany Williams – Intelligence Analyst (Embedded)

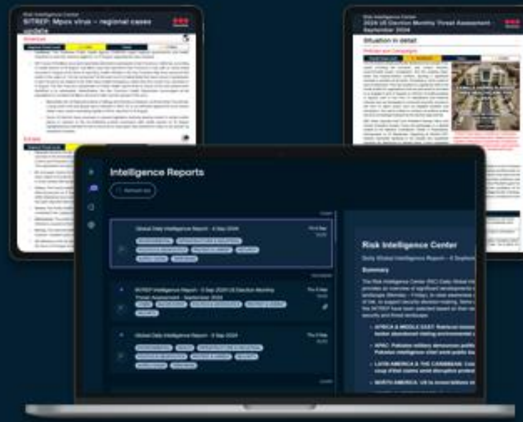
Risk Intelligence Center - Services

Situational awareness intelligence

Awareness

- Reporting the global threat landscape of all industries with +350 reports per year.

Situation Reports   Intelligence Reports



Daily Global Threat Reports

Geo-targeted intelligence

Alerting

- Geo-targeted alerts for security and threat events.

Live email alerts   Threat event details

Location Based Briefs

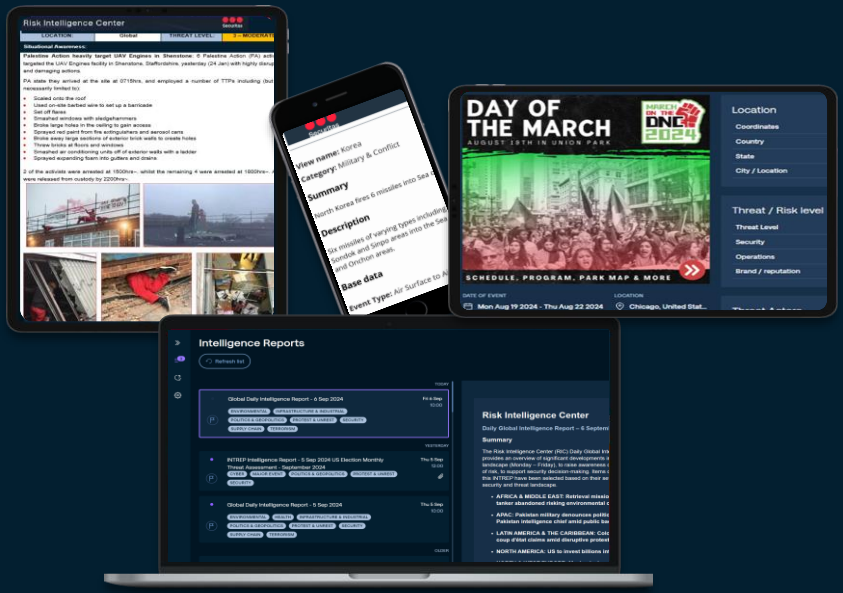
Specific & tailored intelligence

Advisory

- Based on your specific intelligence requirements

Daily monitoring   Specific INTREP

Flash Intelligence Reports



Risk Intelligence Center

LOCATION:	Global	THREAT LEVEL:	3 – MODERATE

Situational Awareness:

Palestine Action heavily target UAV Engines in Shenstone: 6 Palestine Action (PA) acti targeted the UAV Engines facility in Shenstone, Staffordshire, yesterday (24 Jan) with highly disrup and damaging actions.

PA state they arrived at the site at 0715hrs, and employed a number of TTPs including (but necessarily limited to):

- Scaled onto the roof
- Used on-site barbed wire to set up a barricade
- Set off flares
- Smashed windows with sledgehammers
- Broke large holes in the ceiling to gain access
- Sprayed red paint from fire extinguishers and aerosol cans
- Broke away large sections of exterior brick walls to create holes
- Threw bricks at floors and windows
- Smashed air conditioning units off of exterior walls with a ladder
- Sprayed expanding foam into gutters and drains

2 of the activists were arrested at 1500hrs–, whilst the remaining 4 were arrested at 1800hrs–. A were released from custody by 2200hrs–.

View name: Korea
Category: Military & Conflict
Summary
North Korea fires 6 missiles into Sea o
Description
Six missiles of varying types including Sondok and Sinpo areas into the Sea and Onchon areas.
Base data
Event Type: Air Surface to A

DAY OF THE MARCH
AUGUST 19TH IN UNION PARK
MARCH ON THE DNC 2024
SCHEDULE, PROGRAM, PARK MAP & MORE
DATE OF EVENT: Mon Aug 19 2024 - Thu Aug 22 2024
LOCATION: Chicago, United Stat...

Location
- Coordinates
- Country
- State
- City / Location

Threat / Risk level
- Threat Level
- Security
- Operations
- Brand / reputation

Intelligence Reports

Refresh list

TODAY

Global Daily Intelligence Report - 6 Sep 2024 — Fri 6 Sep 10:00
ENVIRONMENTAL · INFRASTRUCTURE & INDUSTRIAL · POLITICS & GEOPOLITICS · PROTEST & UNREST · SECURITY · SUPPLY CHAIN · TERRORISM

YESTERDAY

INTREP Intelligence Report - 5 Sep 2024 US Election Monthly Threat Assessment - September 2024 — Thu 5 Sep 12:00
CYBER · MAJOR EVENT · POLITICS & GEOPOLITICS · PROTEST & UNREST · SECURITY

Global Daily Intelligence Report - 5 Sep 2024 — Thu 5 Sep 10:00
ENVIRONMENTAL · HEALTH · INFRASTRUCTURE & INDUSTRIAL · POLITICS & GEOPOLITICS · PROTEST & UNREST · SECURITY · SUPPLY CHAIN · TERRORISM

OLDER

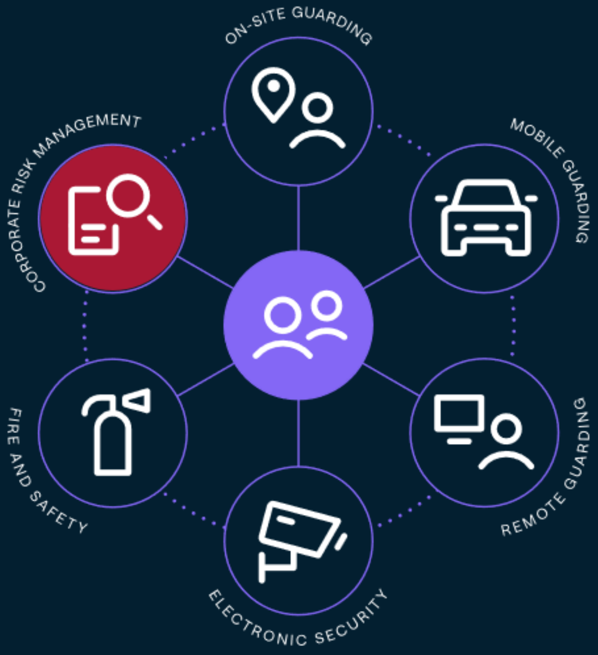
Risk Intelligence Center

Daily Global Intelligence Report – 6 Septem

Summary

The Risk Intelligence Center (RIC) Daily Global Int provides an overview of significant developments i landscape (Monday – Friday), to raise awareness c of risk, to support security decision-making. Items c this INTREP have been selected based on their se security and threat landscape.

- AFRICA & MIDDLE EAST: Retrieval missio tanker abandoned risking environmental c
- APAC: Pakistan military denounces politic Pakistan intelligence chief amid public ba
- LATIN AMERICA & THE CARIBBEAN: Colc coup d'état claims amid disruptive protest
- NORTH AMERICA: US to invest billions in



By utilizing the Risk Intelligence services, you can benefit from:

- Independent Industry-leading expertise
- Tailor-made solutions for your specific requirements
- Specific intelligence to support decision making
- Flexible engagement to maximize impact and investment
- intelligence-led security, added value and peace of mind

Securitas

Contact us:

For intelligence requirements: intelligence@securitas.com

For app enquiries: RIC@securitas.com