Allianz

Sebastian/ Adobe Stock

ALLIANZ COMMERCIAL

Political violence and civil unrest trends 2025

Overview

Businesses have ranked political risks and violence as a top 10 global risk for the past three years the **Allianz Risk Barometer** shows, demonstrating that it has become a key concern for companies of all sizes.

Political violence activity can impact businesses in many ways. In addition to endangering the safety of employees and customers, those in the immediate vicinity of unrest can suffer business interruption losses and material damage to property or assets, while indirect damage can be inflicted on companies in the form of "loss of attraction" or "denial of access" to their premises.

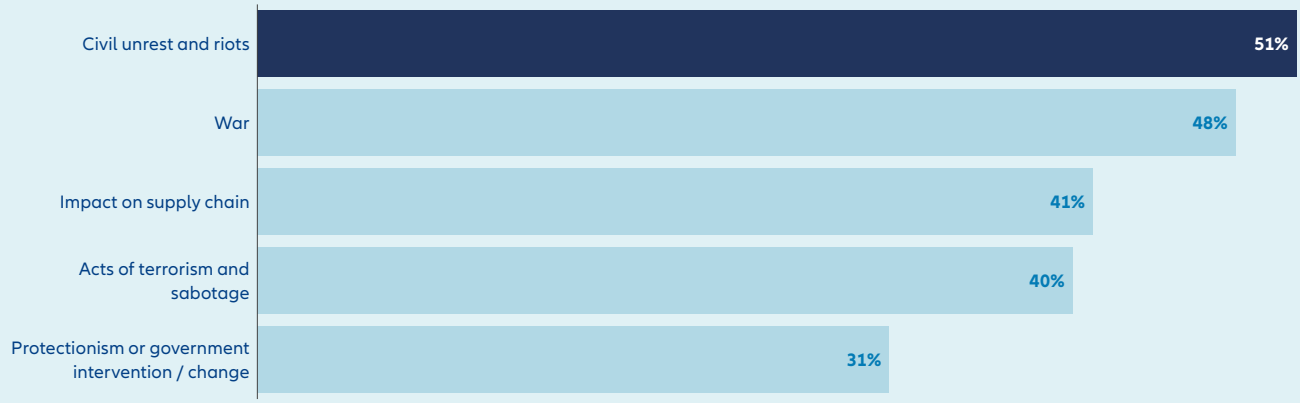
Among the key drivers of company concerns in 2024 were the record-breaking year of elections around the world and the potential for civil unrest during and after these events, as well as the developing conflict in the Middle East and ongoing war in Ukraine. Companies, especially in the large-corp and mid-sized segments have also been watchful of any miscalculation between China and Taiwan possibly escalating into a regional conflict.

Political violence remains a top 10 global business risk according to our customers because politics is increasingly perceived as being dominated by populism and blame and division, geopolitics by nationalism and a changing world order, and economics by mismanagement, corruption, and continually rising disparity between the "super rich", "rich" and the rest.

Ultimately, the speed of change we have seen since 2019, has given companies little time to address their supply chains, meaning they have had to operate in an uncertain environment. Another factor is the unpredictability of the size, location and length of any incidents or issues. Unlike with other perils such as flood or windstorm, it is difficult to prepare in the same way to mitigate losses and build contingency and business continuity plans.

George Khelashvili / Shutterstock

Which political risk and violence exposures are your company most worried about?
Top 5 responses



The impact of civil unrest or strikes, riots and civil commotion (SRCC) is the exposure companies fear most, according to more than half of Allianz Risk Barometer respondents.

Source: Allianz Commercial, Allianz Risk Barometer 2025
Figures represent how often a risk was selected as percentage of all responses.
Respondents: 513
Figures don't add up to 100% as up to three risks could be selected.

Further challenges for businesses in this space through 2025 and beyond are anticipated, as is already evidenced by the major anti-government protest activity seen in the Balkans and Türkiye, for example. Companies are having to deal with this new normal of increasing anti-social behavior and protest activity where events can last for longer and more hostile activism is to be expected. Since 2017, there have been over 800 significant anti-government protests in more than 150 countries, with more than 160 significant events taking place during 2024 alone. 18% of these protests lasted for more than three months. Allianz research shows that in the top 20 countries for frequency of protest and riot activity around the world during 2024, there were more than 80,000 incidents.

The risk of rogue state-sponsored sabotage is also a growing area of concern with covert acts here to stay. Irrespective of any wars ending, the cat is out of the bag. Key infrastructure may often be the primary target, but the risk is actually much broader, with cyber tools enabling state proxies to conduct a wide range of sophisticated and deniable operations. Meanwhile, the increasing frequency of plots and attacks from Islamist groups and inspired individuals, as well as growing empowerment among supporters of other far right and far left groups are among the factors driving the complex global terrorism landscape. This risk really is now shaped by multiple forces.

> In the top 20 countries for frequency of protest and riot activity around the world during 2024, there were more than 80,000 incidents

Ultimately, global stability in 2025 continues to be undermined by the forces of international conflict, geopolitical upheaval and economic uncertainty and the prospect of trade wars. In this report, Allianz Commercial experts highlight some of the potential drivers of political violence and civil unrest activity. Businesses need to remain vigilant about the shapeshifting nature of political violence and mindful of the risk that localized unrest could significantly impact their activities.

Summary – Trends to watch

Contents

Civil unrest – the exposure of most concern

Businesses are more concerned about the disruptive impact of anti-social behavior on their operations than that of any other political violence and terrorism exposure. The impact of civil unrest or strikes, riots and civil commotion (SRCC) activity is the political risk and violence exposure companies fear most, according to the **Allianz Risk Barometer 2025** with more than 50% of respondents globally ranking this as their main worry. It also ranks as the top concern in countries such as Colombia, France, South Africa, the UK and the US, reflecting the fact that incidents around the world are rising in number and lasting for longer.

There have been over 800 significant anti-government protests since 2017 in more than 150 countries, with more than 160 events in 2024 alone[1] – 18% of protests lasting for more than three months. Allianz research shows that in the top 20 countries for frequency of protest and riot activity around the world during 2024, there were more than 80,000 incidents, with India, US, France, Germany, Türkiye, and Spain among the top countries.

It is a view shared by insurers who have seen the SRCC peril increase in frequency and severity. Events such as riots in Chile and South Africa and the Black Lives Matter unrest in the US have resulted in insured losses well in excess of US$10bn over the past decade, surpassing other levels of political violence and terrorism insurance claims. In certain hotspot territories losses can rival or surpass those from natural catastrophes, while in others, although the direct impact may be minor, events can still trigger long- lasting changes in the societies they affect.

All kinds of civil unrest and protest activity remain a problem. Contributing factors such as high inflation, wealth inequality, food and fuel prices, climate anxieties and concerns about civil liberties or perceived assaults on democracy have not eased. After the “super year of elections” around the world in 2024, further post election changes or policy changes by governments will continue to be trigger factors which could cause protests and flashpoints in many countries around the world over the year ahead, as could any economic hardships that result from tit-for-tat tariff wars.

Terrorism risk shaped by multiple forces

The increasing frequency of plots and attacks from Islamist groups and inspired individuals, as well as growing empowerment among other far-right group supporters, are among the factors driving the complex global landscape. A growing concern is the Islamist terrorism threat on the continent of Europe, with an increasing number of attacks or plots happening over the last 12 months. Overall, terrorist attacks jumped by 63% in the West with Europe most affected, doubling to 67[6].

An increase in terrorist attacks from other political extremists motivated by both far-right and far-left ideologies is also expected to be a major threat over the year ahead, with emerging far-right motivated terrorism considered by many to be the most prominent domestic security threat. Analysis shows there were well in excess of 100 reported terrorism and right wing extremist incidents during 2024[10], from groups ranging from Neo-Nazi to anti-immigration, driven primarily by events in the US, followed by Germany. Meanwhile, far-left extremists are increasingly targeting individuals or companies who they see as contributing negatively towards issues such as climate change or inequality. More frequent and severe actions can be anticipated. In addition, extremists are increasingly acting on their own, making them harder to track, disrupt and prevent.

Hybrid threats – state-sponsored sabotage and warfare here to stay

Covert acts of sabotage by state actors such as Russia, Iran and North Korea are high on the risk agenda with the number of alleged incidents on the rise. The rise of authoritarian politics and the weakening of international accountability mechanisms is further emboldening rogue states. Critical infrastructure may be the main target, but the risk is actually much broader. Even if wars such as Ukraine do end "*the sabotage cat is out of the bag*" and the risk is here to stay.

More than three years after Russia invaded Ukraine, the tactics deployed from Moscow have included physical sabotage and cyber-attacks, not forgetting electoral interference. Analysis suggests that almost 200 civilian vessels[13] have engaged in suspected espionage activities in the North Sea near key infrastructure including cutting critical undersea communication cables and damaging pipelines. Water supplies have also been targeted in a number of countries as have logistics companies and transportation infrastructure. Other incidents include a surge in GPS and automatic identification system (AIS) jamming on ships. Not only is the number of incidents increasing, but they are also expanding geographically, with targets shifting westwards from Scandinavia and the Baltics.

New tech versus old tech increases the threat of damage and disruption

Increased digital reliance and geopolitical instability are also heightening the risk of cyber-attacks that inflict physical damage. Attacks on critical infrastructure and physical assets ranks second globally in the most concerning cyber exposures for businesses, according to the **Allianz Risk Barometer,** with concerns growing about vulnerability to disruptions to physical processes, equipment damage, and even safety.

To manage physical processes at many of these large installations complex Industrial Control Systems (ICS) or operational technology (OT) systems are used for control and monitor purposes. In many cases, these systems are legacy in nature. For example, in refinery operations manipulation of ICS and safety systems could lead to a catastrophic fire or cause environmental damage.

Environmental activism turns more hostile

With many countries changing their net zero promises and some companies announcing a shift back towards fossil fuels, environmental activism is being galvanized like never before, continuing a recent trend which saw incidents increase by around 120% between 2022 and 2023[25]. Increasingly, the activity of climate protestors is entering a new phase of disruption, which is becoming more militant, deploying more targeted tactics against those companies or organizations they see as being responsible for climate breakdown worsening, ensuring environmental protests are escalating from acts of violence to larger criminal acts. This escalation risk cannot be ignored, particularly given the fact that such attacks can be challenging to prevent or disrupt.

Risk management and insurance

The sustained political violence and SRCC activity in evidence around the world is a challenge not only for businesses but also for the broader insurance market because the coverage goes well beyond the political violence and terrorism class of business. Almost all property classes of insurance offer some degree of SRCC coverage.

As unrest can now spread more quickly and widely – thanks in part to the power of social media – economic and insured losses from such activity can be considerable. The patterns of protests and violence over the last 10 years has shown that targets such as government buildings, transport infrastructure, retail premises and distribution centers for critical goods can be specific but, often, businesses are victims of their locality and their footprint.

Companies need to be alive to the shapeshifting nature of political violence risk and protect their people and property with forward planning, such as ensuring safe and robust business continuity planning is in place in event of an incident, increasing security and reducing or relocating inventory if they are highly likely to be affected by an event. Using scenario planning and tracking risks in areas key to their operations, particularly transport and manufacturing centers, can raise businesses' awareness of where political violence risk might be intensifying.

Organizations also need to review their insurance. Property policies may cover political violence claims in some cases, but insurers also offer specialist protection. Businesses with multi-country exposures are showing more interest in political violence coverage but there is also greater engagement from the SME and mid-corp space about these risks, a true reflection of increasing concern in this segment.

Political violence and civil unrest: the impact on business

As unrest can now spread more quickly and widely – thanks in part to the power of social media – financial costs are mounting. Economic and insured losses from such activity can be considerable, resulting in significant losses for companies and their insurers.

The pattern of protests and violence over the last 10 years has clearly shown that some industries and occupancies are much more vulnerable to the full spectrum of political violence perils. Sometimes targets can be specific but, often, businesses are victims of their locality and their footprint.

Buildings and businesses most at risk

Targets can vary depending on the type of incident but can include:

- **Government, municipal, army or police buildings** or infrastructure
- **Transport infrastructure** and hubs
- **Retail premises,** particularly those with high value assets; pharmacies; those that are foreign-owned or represent globalization and/or the economic interests of a former colonial power
- **Private enterprises,** including those that are foreign-owned or believed to have supported an unpopular government
- **Critical assets,** such as petrol stations, or those of high value
- **Distribution centers** for critical goods and assets
- **Tourism and hospitality businesses,** including those in countries that international governments have deemed inadvisable for non-essential travel
- **Supply chains –** if disrupted, this could lead to resource nationalism as governments attempt to ensure supply of essential goods to their own countries.

A rising risk for smaller companies too

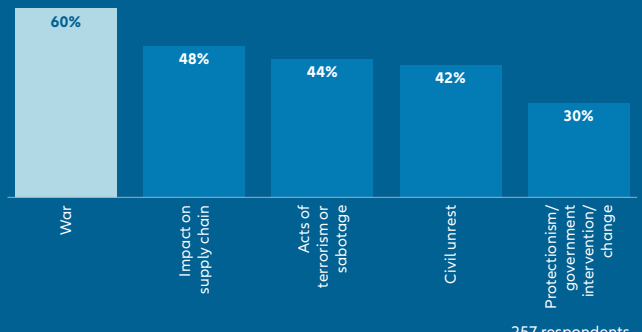
Political risks and violence is a risk riser for larger companies (US$500mn+) around the world in the **Allianz Risk Barometer 2025,** up to #7 from #8 year-on-year. However, it is also a new entry in the top 10 risks for smaller companies (<US$100mn) at #10 and ranks #9 for mid-size companies (>$100mn to $500mn) globally.

Political violence events can potentially have a much bigger impact on smaller and mid- sized business compared with large multinationals for a number of reasons. Such companies tend to have a smaller footprint or a more regionalized focus which means that if their location is experiencing difficulty, it is much harder for them to mitigate potential risks such as damage to property, business interruption or disruption to supply chains and customers. They also have smaller budgets for risk management activities and to find alternative buyers or customers or relocate production.

Which political risk and violence exposures are your company most worried about?

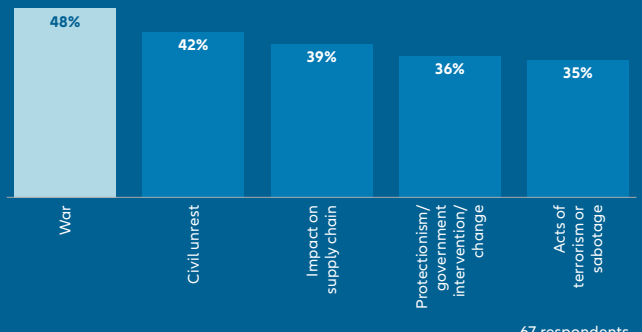
By region

Europe



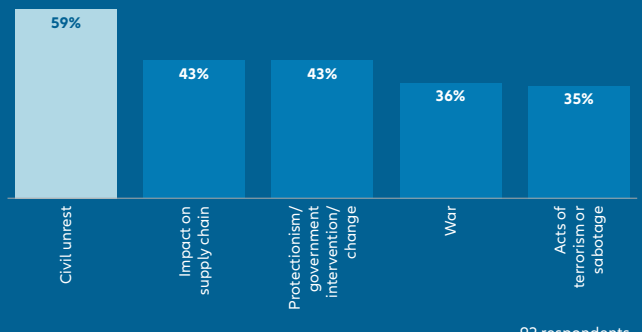
257 respondents

Asia Pacific



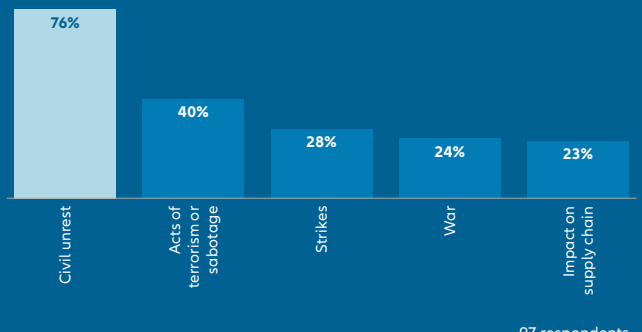
67 respondents

Americas



92 respondents

Africa and Middle East



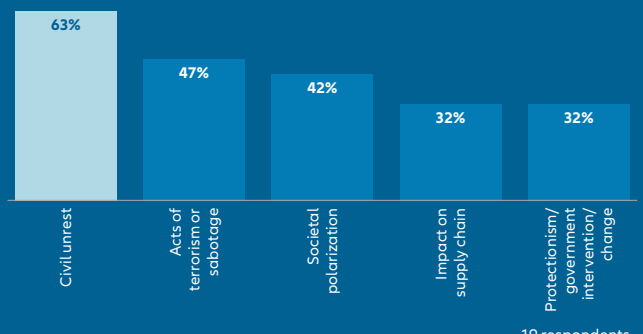
97 respondents

Source: Allianz Commercial, Allianz Risk Barometer 2025

Which political risk and violence exposures are your company most worried about?

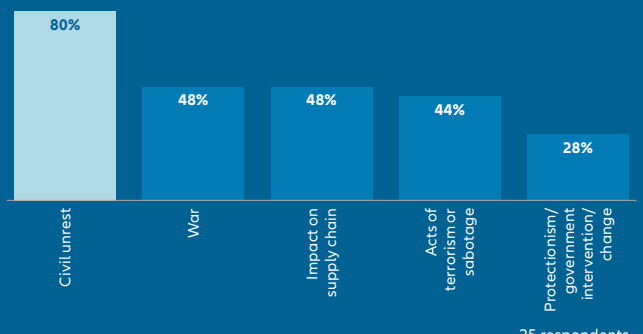
By selected countries

Colombia



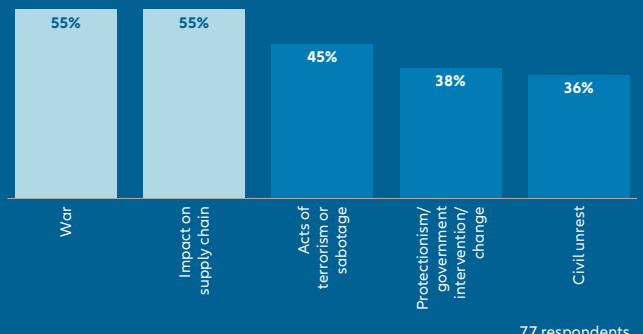
19 respondents

France



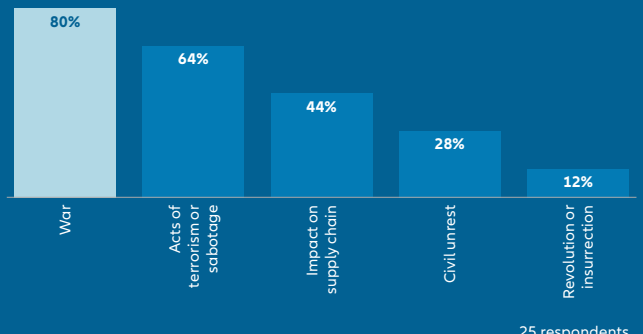
25 respondents

Germany



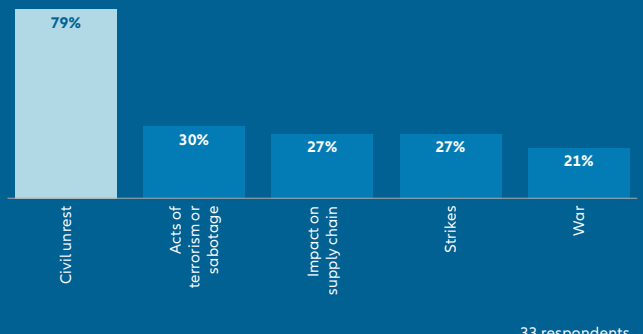
77 respondents

Italy



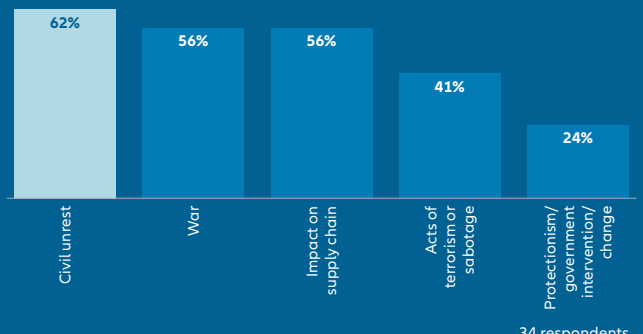
25 respondents

South Africa



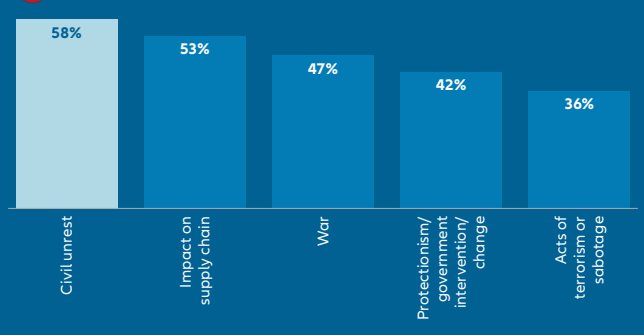
33 respondents

UK



34 respondents

US



45 respondents

Source: Allianz Commercial, Allianz Risk Barometer 2025

Sohan Nuhoglu / Shutterstock

TRENDS

Civil unrest – the exposure of most concern

Businesses are more concerned about the disruptive impact of anti-social behavior on their operations than that of any other political violence and terrorism exposure.

The impact of civil unrest or strikes, riots and civil commotion (SRCC) is the political risk and violence exposure companies fear most, according to the **Allianz Risk Barometer 2025** with more than half of respondents globally ranking this as their main worry. It also ranks as the top concern in countries such as Colombia, France, South Africa, the UK and the US, reflecting the fact that incidents around the world continue to increase and are lasting for longer. There have been over 800 significant anti-government protests since 2017 in more than 150 countries, with more than 160 events in 2024 alone, according to the Carnegie Endowment Global Protest Tracker[1] – 18% of protests having lasted more than three months. Allianz research shows that in the top 20 countries for frequency of protest and riot activity around the world during 2024, there were more than 80,000 incidents[2].

"It is a view also shared by insurers as we have seen this peril increase in frequency and severity over the last six years in particular," says **Srdjan Todorovic, Head of Political Violence and Hostile Environment Solutions, Allianz Commercial.** *"For example, the SRCC peril, and events such as riots in Chile and South Africa and the Black Lives Matter unrest in the US have resulted in insured losses well in excess of US$10bn over the past decade, surpassing other levels of political violence and terrorism insurance claims. In certain hotspot territories losses can rival or surpass those from natural catastrophes but in others, although the direct impact can be minor, events can still have long-lasting changes in the societies they affect."*

Of course, 2024 was billed as the "Super Year of Elections", with as much as half of the world's population estimated to have gone to the polls before the year was out. There was much concern globally about the number of elections and their potential for political violence and civil unrest activity, particularly in the US. However, although there were some significant events and losses in the SRCC space, such as in the UK, Kenya, New Caledonia, and South Korea for example, these were not directly linked to the results of elections.

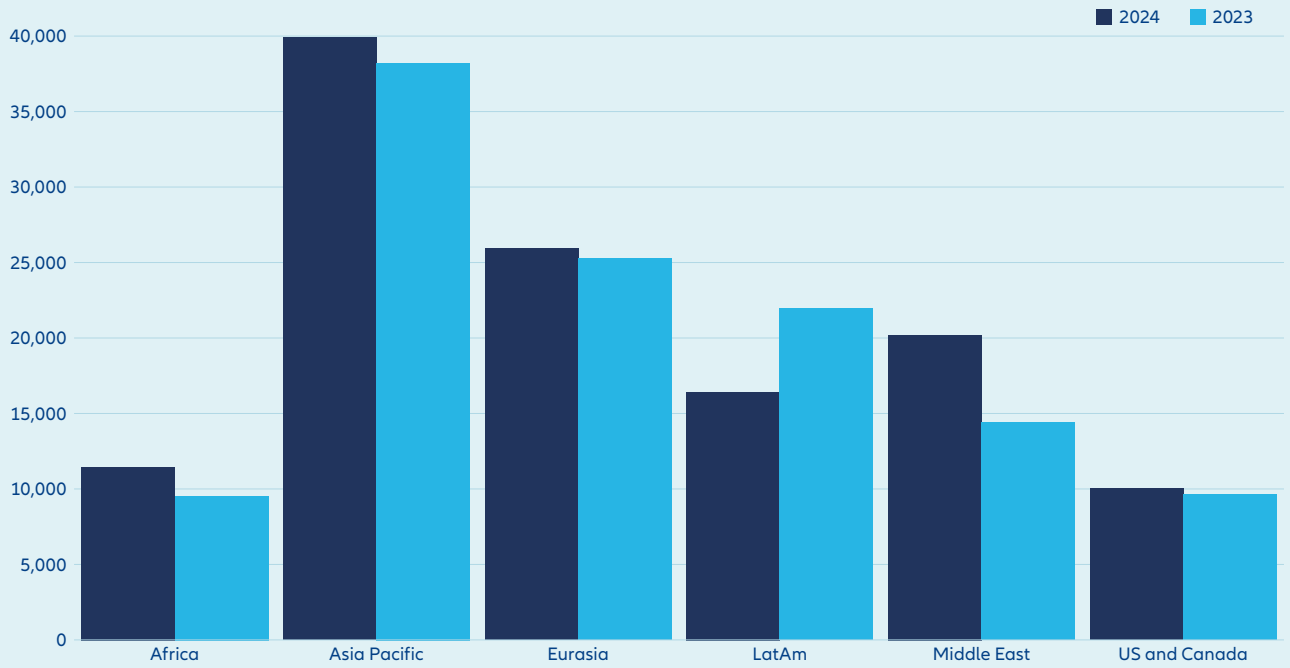
Rather, political policy shifts and changes were the key drivers for protests, riots and loss activity. In Kenya, an increase in taxes on food, as well as on other sectors of the economy to help repay foreign loans and fund development programs saw protestors take to the streets and storm and set fire to parliament buildings, forcing the government to back down[3].

In May 2024, protests and riots broke out in New Caledonia, a *sui generis* collectivity of overseas France in the Pacific Ocean where proposed changes to voting rules were the catalyst for unrest that resulted in at least 13 deaths, the declaration of a state of emergency, deployment of the French army, the block of the social network TikTok, and estimated insurance industry losses in excess of $1bn to date.

Economic circumstances also resulted in violence in other parts of the world, such as in the French Caribbean territory of Martinique where protests spread in September 2024 and resulted in gunfire, injuries, buildings and cars being set on fire, and shops being looted in response to the high cost of living (Martinique residents pay around 30% more for food compared with mainland France).

Number of protests and riots by region

2023-2024 (January-early October)



All regions around the world, with the exception of Latin America, saw a year-on-year increase in the number of protests and riots during 2024.

Sources: Armed Conflict Location and Event Data (Acled), Allianz Research

Top 20 countries by frequency of protests and riots in 2024

Rank	Country	2024	2023	Difference
1	India	18,626	15,373	↑ 21.2%
2	US	8,549	8,383	↑ 2%
3	France	5,517	7,045	↓ 21.7%
4	Pakistan	5,405	5,380	↑ 0.5%
5	Mexico	4,921	4,989	↓ 1.4%
6	Germany	4,068	2,994	↑ 35.9%
7	South Korea	3,931	5,015	↓ 21.6%
8	Türkiye	3,729	2,089	↑ 78.5%
9	Spain	2,933	2,264	↑ 29.6%
10	Morocco	2,857	934	↑ 205.9%

Rank	Country	2024	2023	Difference
11	Iran	2,815	2,088	↑ 34.8%
12	Indonesia	2,664	2,315	↑ 15.1%
13	Bangladesh	2,223	1,458	↑ 52.5%
14	Italy	2,218	2,366	↓ 6.3%
15	Kenya	2,068	1,311	↑ 57.7%
16	Colombia	1,666	2,070	↓ 19.5%
17	Canada	1,577	1,381	↑ 14.2%
18	South Africa	1,544	1,505	↑ 2.6%
19	Japan	1,531	1,290	↑ 18.7%
20	Poland	1,441	713	↑ 102.1%

India, Germany, Kenya, Poland, Morocco and Türkiye were among the countries who experienced significant increases in the frequency of protest and riot activity during 2024.

Sources: Acled, Allianz Research. This does not include countries where conflict is ongoing (Yemen, Palestine). Count of events from 01 January to 04 October of each year.

Meanwhile, social media and misinformation played a major role in civil unrest activity escalating in different parts of the UK during 2024, following a number of fatal stabbings at a children's dance class in July. Speculation online that the suspect was an illegal migrant led to demonstrations in more than 20 towns and cities, resulting in violent disorder. Insured losses from these events are estimated in the low hundreds of millions of pounds. Thousands of people were arrested and hundreds imprisoned. A number of jail terms were handed down for social media posts.

There continue to be a number of protests and strikes in many other countries including Argentina (where policy changes led to increased anti-government protests), France (farmers protesting against low food prices, the removal of fuel subsidies and a free trade agreement) and Serbia, where protests against the government spread to more than 400 cities and towns, and started to incorporate other issues, after the collapse of a railway station in November 2024, to name just a few. Meanwhile, in March 2025, huge protests broke out in Türkiye after Istanbul's Mayor, Ekrem Imamoglu, was detained on corruption charges[4]. Türkiye had already experienced a close to 80% year-on-year increase in the frequency of protest and riot activity during 2024, according to Allianz research, ranking it in the top 10 countries in the world.

> Further post election changes or policy changes by governments will continue to be trigger factors

"All kinds of civil unrest and protest activity remains a problem, weighing heavily on the minds of businesses around the globe. Contributing factors such as high inflation, wealth inequality, food and fuel prices, climate anxieties and concerns about civil liberties or perceived assaults on democracy have not eased. Further post election changes or policy changes by governments will continue to be trigger factors which could cause both low-level protests and flashpoints in many countries around the world over the year ahead, as could any economic hardships that result from tit- for-tat tariff wars," says **Etienne Cheret, a Regional Head of Political Violence and Terrorism at Allianz Commercial.**

Studio MDF / Shutterstock

TRENDS

Terrorism risk shaped by multiple forces

The increasing frequency of plots and attacks from Islamist groups and inspired individuals, as well as growing empowerment among other, emerging, far right group supporters and populist movements are among the factors driving the complex global landscape.

During 2024 Islamic State (IS) and its affiliates expanded its operations causing more than 1,800 deaths in 22 countries, according to Vision of Humanity's Global Terrorism Index[5], remaining the deadliest terrorist organization.

The global threat posed by Sunni militant extremists is expected to increase further over the year ahead, driven by the humanitarian crises in the Middle East and Gaza and Lebanon.

A growing concern is the terrorism threat in Europe, with an increasing number of attacks or plots happening over the last 12 months. Terrorist attacks jumped by 63% in the West with Europe most affected, doubling to 67, according to the index, including attacks by IS and Hamas [6]. Last year, the risk around large events such as the Euros football tournament, the Olympics and Paralympic Games, and even Taylor Swift's record-breaking world music tour led to enhanced policing and security as well as the cancellation of shows.

Newer groups like ISIS-K, the Islamic State Khorasan Province, are looking at high profile targets with mass casualties, such as the tragic attacks on the Crocus City Hall in Moscow in March 2024, which resulted in more than 140 casualties and numerous injuries, making it one of the deadliest terrorist attacks in Europe.

Meanwhile, power vacuums in the Middle East, such as the fall of the Assad regime in Syria, could also enable militant extremist organizations to grow and expand over the coming year.

An increase in attacks from other groups of political extremists motivated by both far-right and far-left ideologies is also expected to be a major threat over the year ahead. Some UN member states already consider emerging forms of far-right terrorism to be the fastest growing or even most prominent domestic security threat they face, according to a Report of the Secretary General[7].

Attacks by such far-right groups and organizations, whether they be Neo-Nazi, white supremist, antisemitic or anti-immigration focus seek to create divisions in society. In July 2024, the EU added the group The Base[8], a networked organization formed in the US which adheres to the usage of political violence or terrorism *"in pursuit of the destruction of the physical manifestations [of..] modernity, liberalism, and capitalism[9]"* to its list of terrorist entities, the first far-right entity to be listed. It is already designated as a terrorist organization by countries such as Canada, the UK and Australia.

Analysis shows there were well in excess of 100 reported terrorism and right wing extremist incidents during 2024, driven primarily by events in the US, followed by Germany, despite its anti-Nazi laws[10]. The US also saw a 200% rise in antisemitic incidents[11]. Australia also reported high levels of far-right violence, driven by domestic tensions, with the UK, France and Spain also seeing activity. Incidents in countries such as Argentina and Canada also marked the spread of far-right extremism into regions traditionally less impacted by such developments.

Meanwhile, far-left extremists are increasingly targeting individuals or companies who they see as contributing negatively towards issues such as capitalism, climate change or inequality. More frequent and severe actions during 2025 and beyond can be anticipated.

"In addition, political extremists are increasingly acting on their own, ensuring they are harder to track, disrupt and prevent. Technology has made it easier to plan and carry out such attacks in isolation, which means this is one of the most unpredictable terrorist threats today," **Srdjan Todorovic, Head of Political Violence and Hostile Environment Solutions, Allianz Commercial,** explains.

Stephen / Adobe Stock

Over the last 12 months terrorist attacks in the West jumped by

63%

The number of attacks in Europe doubled to

67

Halfpoint / Adobe Stock

TRENDS

Hybrid threats – state-sponsored sabotage and warfare here to stay

Covert acts of sabotage will likely remain, irrespective of current wars ending, with the number of alleged incidents on the rise. Key infrastructure may be the main target, but the risk is actually much broader.

The threat of state-sponsored sabotage on private sector assets is a big concern for the year ahead and beyond. The rise of authoritarian politics and the weakening of international accountability mechanisms is further emboldening rogue states.

As Russia has continued its invasion of Ukraine, it has wanted to hurt Western countries for their continued support for Kyiv. Private sector assets in European countries, particularly anything related to critical infrastructure or the defence-industrial base, are likely to be among Russia's primary targets.

Even if the war in Ukraine does end the *"sabotage cat is out of the bag"* and the risk is here to stay, according to **Srdjan Todorovic, Head of Political Violence and Hostile Environment Solutions, Allianz Commercial.** And although this might appear to concern businesses in certain sectors more than others, especially those with offshore assets, like oil and gas, telecommunications, and power/utilities, the risk is actually much broader.

"This represents a real threat for any businesses in the line of fire, as well as the commercial insurance industry across lines of cover including property, business interruption, cyber, war, political violence and terrorism," says **Todorovic.**

The risk of a broadening front for covert acts of sabotage by state actors such as Russia, Iran and North Korea will likely increase


Tom Woollard / Adobe Stock

Last year saw a dramatic rise in documented Russian hybrid sabotage/warfare activities across Europe. The number stood at 44 incidents, up from just 13 in 2023, according to research from Leiden University[12], with the real number likely even higher. Not only is the number of incidents increasing, but they are also expanding geographically, with targets shifting westwards from being previously concentrated in Scandinavia and the Baltics.

More than three years after Russia invaded Ukraine, the tactics deployed from Moscow have included physical sabotage and cyber-attacks, not forgetting electoral interference. Analysis suggests that almost 200 vessels[13] have been suspected of engaging in espionage activities in the North Sea near key infrastructure including cutting critical undersea communication cables and damaging pipelines.

Water supplies have also been targeted in Finland, Germany and Sweden[14], while sabotage questions were also raised around a number of recent events involving logistics company DHL in Birmingham, UK (a package fire in a warehouse)[15] and in Leipzig, Germany (a cargo plane crash)[16]. Other incidents include a surge in GPS and automatic identification system (AIS) jamming on vessels in the Baltic Sea.

"As war in Ukraine continues, and as key allies of Russia continue to suffer meaningful losses (for example, the overthrow of former President Bashar al-Assad in Syria) the risk of a broadening front for covert acts of sabotage by state actors such as Russia, Iran and North Korea will likely increase. Unfortunately, there is no quick and easy solution to halting these hybrid attacks," says **Todorovic.**

TRENDS

New tech versus old tech increases the threat of rogue state-triggered damage and disruption

Increased digital reliance and geopolitical instability are also heightening the risk of a range of sophisticated and deniable cyber-attacks.

Advances in technology and global connectivity have increased production and dissemination of misinformation and disinformation. To sow discord, Advanced Persistent Threat (APT) actors, which are usually sponsored by rogue nations or organizations, leverage cyber-attacks to disseminate false information, using techniques such as manipulated online news platforms and compromised social media accounts to instigate real-world events such as aggravating political polarization, promoting social unrest and riots and undermining democratic elections.

APT groups often engage in sophisticated cyber espionage, such as in the case of the Southport attacks and subsequent far-right riots during 2024 in the UK, which spread disinformation, and caused social disruption.

Increased digital reliance and geopolitical instability are also heightening the risk of cyber-attacks that inflict physical harm at the same time, according to **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.**

When cyber attacks critical infrastucture

- During the Covid-19 pandemic, APT actors exploited unpatched software vulnerabilities and used password spraying attacks to infiltrate organizations. Targets included healthcare bodies, pharmaceutical firms, academia, medical research institutions, and local governments. The goal was to gather intelligence on healthcare policies and access sensitive Covid-19 research for commercial and state advantage.
- The FBI reported that the North Korean-linked TraderTraitor group was behind the $1.5bn hack of crypto exchange Bybit in February 2025[17]. Such large-scale theft disrupts financial markets, erodes trust in institutions, and contributes to economic instability, potentially fuelling social unrest and political violence. Additionally, North Korea's cyber crimes fund activities that threaten international security and heighten geopolitical tensions, increasing the risk of cyber warfare.
- In April 2024, the hacktivist group known as the Cyber Army of Russia Reborn, claimed responsibility for cyber-attacks targeting water utility control systems in the Texas towns of Abernathy and Muleshoe as well as Indiana's Tipton West Wastewater Treatment Plant[18], by releasing videos demonstrating how they allegedly manipulated human-machine interfaces (HMIs) used to regulate these utilities.
- A ransomware attack on the Colonial Pipeline in 2021 resulted in it shutting it down for several days impacting consumers and airlines along the US East Coast[19].
- Even back in 2015, cyber-attacks using BlackEnergy malware led to massive power outages in Western Ukraine, affecting around 225,000 people[20]. Attributed to Russian state-sponsored actors, these incidents highlight the vulnerability of critical energy infrastructure to cyber threats.

Critical infrastructure, including energy, transportation, and manufacturing, faces growing vulnerability to disruptions, equipment damage, and threats to human safety via cyber means.

To manage physical processes at these large installations complex Industrial Control Systems (ICS) or operational technology (OT) systems are used for control and monitor purpose. *"Typically, these systems are legacy in nature and have obsolescence issues. That means they are vulnerable to attacks that can disrupt physical processes which can lead to potentially hazardous scenarios,"* **Baviskar** explains.

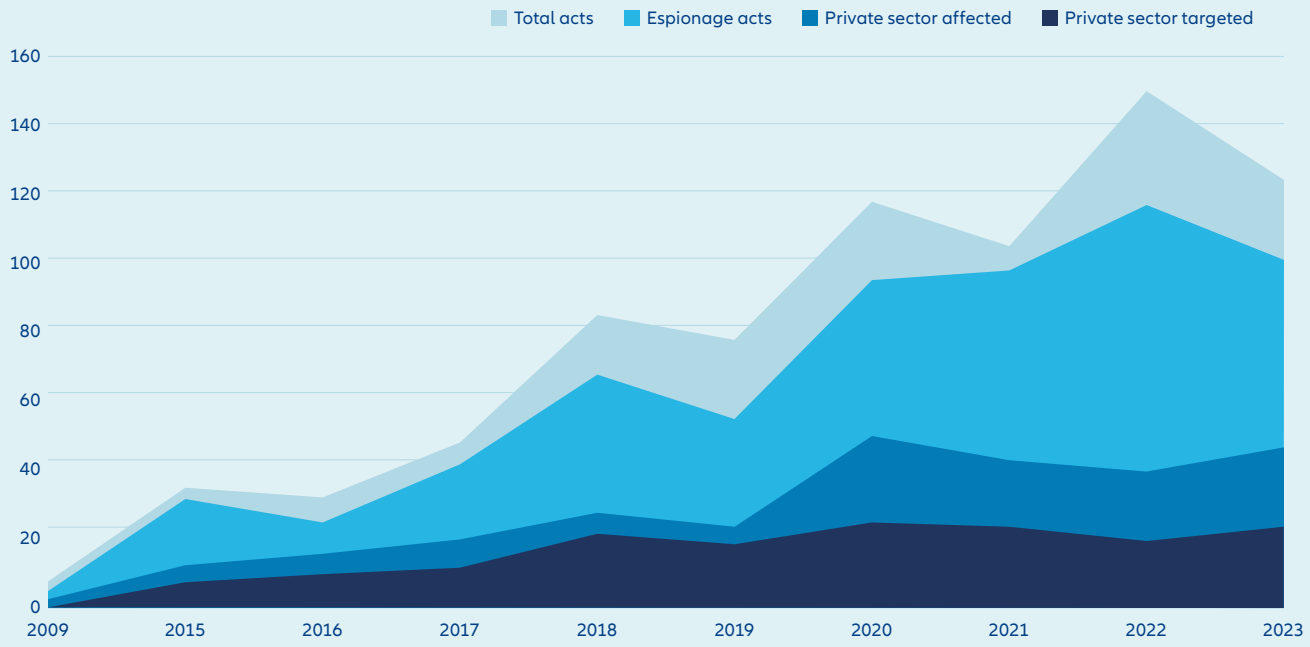
For example, in refinery operations manipulation of ICS and safety systems can lead to catastrophic fire, explosions and can cause major environmental damage due to hydrocarbon releases.

Utility companies too depend extensively on OT systems. The prevalence of outdated, internet-unsecured devices within such networks poses a major security challenge due to infrequent updates.

The utility sector's cyber security weaknesses render it highly vulnerable. Exploiting internet-accessible OT and ICS devices, including those in the wastewater and water sectors could affect millions of people, with potentially severe consequences for public health and safety, says **Baviskar.**

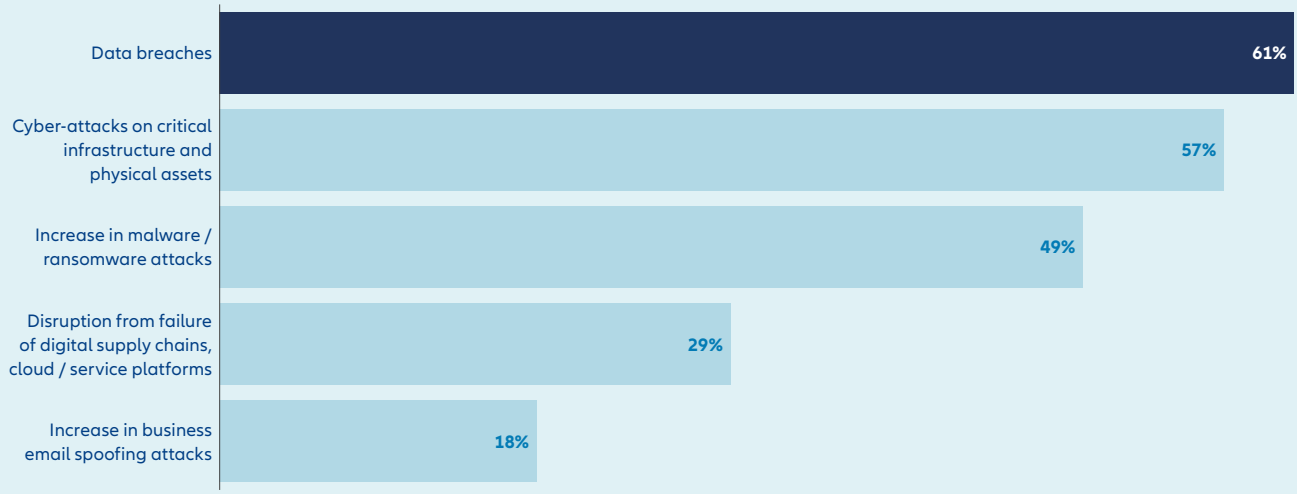
The vulnerability of transportation systems to cyber threats also raises critical concerns regarding the potential for cyber-physical attacks to cause tangible damage. While modern aircraft possess strong security protocols, vulnerabilities within airport infrastructure, including baggage handling and air traffic control, present a tangible risk of physical damage stemming from cyber-attacks. Cyber-attacks targeting other transportation infrastructure also pose a significant risk of physical damage, with disruptions to signaling systems capable of triggering collisions or derailments. In August 2023, a cyber-attack on Poland's railway system[21], where hackers manipulated unsecured radio signals to activate emergency train stops, demonstrates the susceptibility of outdated infrastructure to digital threats.

Increase in state-sponsored cyber operations worldwide



Source: European Commission, Outsmart malicious actors to deter hybrid attacks, Safer Together.
Based on EUISS, 2024, and Council on Foreign Relations, Cyber Operations Tracker, 2024.

Which cyber exposures concern your company most?
Top 5 responses



Attacks on critical infrastructure and physical assets ranks second globally in the most concerning cyber exposures for businesses.

Source: Allianz Commercial, Allianz Risk Barometer 2025
Figures represent how often a risk was selected as percentage of all responses
Respondents: 1,450
Figures don't add up to 100% as up to three risks could be selected.

Assessing the robustness of cyber security for key infrastructure demands a multi-faceted approach, **Baviskar** explains:

"At Allianz we engage in client discussion through cyber risk dialogue to discuss potential threats to the industry, as well as the insured's weaknesses in people, technology and processes. Beyond traditional IT defenses, evaluations also include scrutinizing vulnerabilities, including legacy systems which are often ill-equipped for modern cyber threats, as well as an end-to-end assessment of the insured's value chain."

Key weaknesses often reside in unpatched, poorly secured legacy systems, and the convergence of IT and OT networks. Supply chain vulnerabilities, inadequate incident response plans, and a lack of robust security awareness training further exacerbate these risks. Human error, particularly in access management and patching protocols, remains a significant entry point for malicious actors.

"The convergence of Artificial Intelligence, social media, phishing, and Business Email Compromise attacks creates a potent and evolving threat landscape," says **Baviskar.** "*These technologies are being weaponized to create more convincing and effective cyber-attacks."*

How an organization will recover and maintain critical functions during and after a disruption is key. A robust business continuity plan encompasses a business impact analysis to pinpoint critical functions, defined recovery strategies and procedures, clear communication protocols, reliable data backup and recovery systems, flexible alternative work arrangements, and regularly conducted testing and exercises. Comprehensive audits encompass physical security, incident response protocols, and supply chain resilience. Regular penetration testing and threat intelligence integration are also crucial for identifying and mitigating emerging risks, ensuring the continuous protection of essential services, **Baviskar** concludes.

Brian Minkoff / Shutterstock

TRENDS

Environmental activism turns more hostile

With many countries changing their net zero promises and some companies announcing a shift back towards fossil fuels, environmental activism is also being galvanised like never before.

2024 was the hottest year on record according to the World Meteorological Organization (WMO)[22] and the end of the year also brought fears that the global commitment to transition away from fossil fuels was also losing momentum with the growth of the clean energy transition slowing down while burning of fossil fuels continues to rise.

The new US president Donald Trump has confirmed the country's withdrawal from the Paris climate agreement, the world's most important effort to tackle rising temperatures, for the second time, saying he will "drill, baby, drill",[23] ramping up fossil fuel extraction as part of so-called new age of oil and gas exploration. A number of other countries have also signified they will move in a similar direction or have said they will revise or have already revised climate commitments for fiscal ends[24]. At the same time, a number of energy giants have announced significant cuts to the amount they intend in invest in renewable energy, while also announcing they intend to increase oil and gas production.

Environmental protests are escalating from acts of nuisance to larger criminal acts

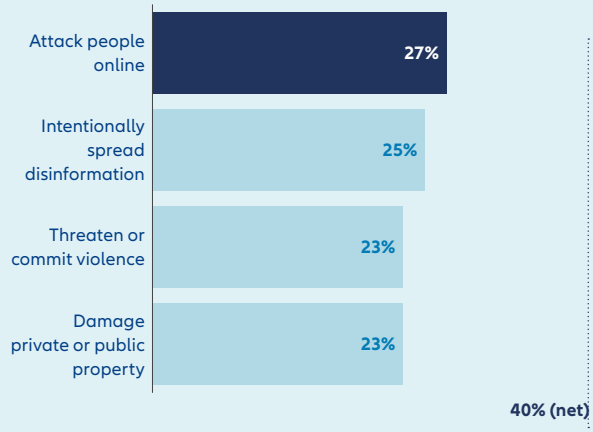
It is little surprise then the area of environmental activism is also expected to heat up over the next year, continuing a recent trend which saw environmental activism incidents increase by around 120% between 2022 and 2023, according to risk intelligence firm Seerist[25]. Increasingly, the activity of climate protestors is entering a new phase of disruption, carrying out acts of sabotage or taking direct action against those companies or organizations they see as being responsible for climate breakdown worsening.

In Berlin, Germany, a left-wing extremist group called Vulkan claimed responsibility for an arson attack on an electricity pylon, which suspended production at a local Tesla plant in March 2024, leading to economic losses estimated in the hundreds of millions of euros[26]. Others staged attacks against gas pipelines and escalated a campaign against concrete with two arson attacks on a Cemex plan in Berlin[27]. In the UK, the Shut The System group claimed that they had cut off the internet to hundreds of insurance companies after severing fibre optic cables[28]. Meanwhile, France is seen as one of the leading countries when it comes to "next level" climate activists with actions ranging from setting fires to full-scale riots to protest against developments such as new motorways and other construction projects.

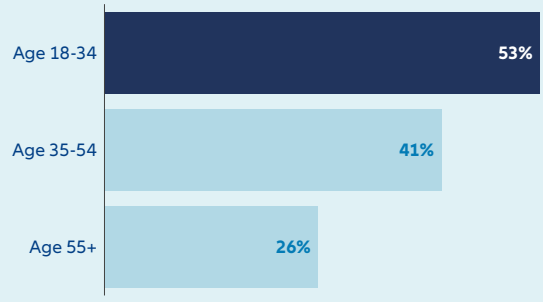
"Government inaction over climate policies or the rowing back on net-zero commitments are certainly galvanizing this new phase of environmental activism which is becoming more militant and deploying more targeted tactics, ensuring that environmental protests are escalating from acts of nuisance to larger criminal acts. This escalation risk cannot be ignored, particularly given the fact that such attacks can be hard to prevent or disrupt," says **Srdjan Todorovic, Head of Political Violence and Hostile Environment Solutions, Allianz Commercial.**

4 in 10 see hostile activism as a viable means to drive change

I approve of hostile activism to drive change



Over 1 in 2 young adults approve of hostile activism



Source: 2025 Edelman Trust Barometer. CNG_MECH. Which actions would you approve of as ways to bring about societal changes you felt would give you and your family a better future? For each of the potential ways to bring about change listed below, pick the statement which best describes how you would feel if someone did this. 4-point scale, codes 3-4, approve. Question asked of half the sample. General population, 28-mkt avg., and by age. The "Hostile Activism" data is a net percentage of attributes 7-10, meaning the percentage of respondents who approved of one or more of the four items shown.

Risk management and insurance

Move fast to protect your people and property in times of upheaval.

The sustained political violence and strikes, riots and civil commotion (SRCC) activity in evidence around the world is a challenge not only for businesses but also for the broader insurance market because the coverage goes well beyond the political violence and terrorism class of business, says **Tim McGain, a Regional Head of Property at Allianz Commercial.**

"Almost all property classes of insurance offer some degree of strikes, riots, and civil commotion coverage. The recent history of protests in Chile, South Africa, France, and in connection with the Black Lives Matter movement have demonstrated yearly the potential severity and impact of this peril."

"Interest for political violence coverage continues to increase. Businesses with multi-country exposures are showing a greater interest in political violence coverage but we are also seeing greater engagement from the SME and mid-corp space about these risks, a true reflection of increasing concern in this segment."

Risk mitigation processes

Political violence risks are not just financial but can also impact operatives who work in or close to high-risk areas, operations, reputations and supply chains. So, what can companies do to safeguard their assets and ensure business activities can continue? Allianz Commercial risk experts suggest considering the following steps when you first spot signs of any unrest or political violence that could impact your business.

- ✓ **Stay abreast of news on planned protests and government policies and implement a business continuity plan (BCP)** in advance if you do not have one in place already
- ✓ **Revise and update your BCP if needed.** Your BCP and your business processes might need amending if a regime introduces new requirements or if there is a risk of sanctions
- ✓ **Retail businesses on the high street should increase security and/or reduce inventory,** including those with high-value assets, those that are multinational or foreign-owned, petrol stations, pharmacies, and banks. Consider temporary relocation of inventory or assets if you are highly likely to be affected
- ✓ **Implement increased security measures at distribution centers**

  Prepare for moving more services online to support business continuity
- ✓ **Protect your supply chains** by ensuring diversity of geography and companies
- ✓ **Review your insurance policies.** Property policies may cover political violence claims in some cases, but insurers also offer specialist coverage to mitigate the impact of strikes, riots and civil commotion via the specialist political violence market.

*"Business interruption has been ranked as a top two risk for the past decade in our annual **Allianz Risk Barometer**. Its causes can range from natural catastrophes to man-made causes and malicious risks including political violence, terrorism, sabotage or cyber events, sanctions, tariffs, trade wars and actual wars.*

"It would therefore be negligent for large companies to not consider political violence and terrorism exposures in the same vein as they are considering the impact that natural catastrophes might have on their operations. Political violence perils need to be factored into business interruption, continuity and planning," concludes **Srdjan Todorovic, Head of Political Violence and Hostile Environment Solutions, Allianz Commercial.**

Comparing political violence and terrorism insurance: what's what?

There are various types of insurance available to cover different political violence risk scenarios. Regardless of which type is selected, all political violence and terrorism insurance types can include the following main coverages:

Property coverage

- Physical damage/losses sustained from an insured peril

Business interruption/Contingent business interruption (CBI) coverage

- Reduction to gross/net earnings suffered due to the necessary interruption of a business' operations; and expenses incurred in attempting to reduce loss or increase operations elsewhere. Denial of access due to civil or military authority; supply chain issues

Standalone terrorism and sabotage insurance

- Act of terrorism: An act or series of acts, including the use of force or violence, by any person or group(s) of persons whether acting alone or on behalf of any organization(s) committed for political, religious or ideological purposes
- Sabotage: Any wilful physical damage or destruction perpetrated for political reasons by known or unknown person(s)

Note: "Full" political violence insurance typically includes all of the above. Coverage for any of the above could include physical damage, BI, CBI, denial of access, delay in startup and advanced loss of profit for construction projects, for example.
Terms of coverage depend on your individual policy.

Standalone strikes, riots and civil commotion insurance

- Strikes: Any wilful act of any striker/ locked-out worker during a strike; any act of a lawful authority to suppress or minimize the strike's consequence
- Riots, civil commotions: Any political act committed in the course of a disturbance of the public peace by a group of persons; any act of a lawful authority's act to suppress or minimize a riot
- Malicious damage: Physical loss/damage resulting from a malicious political act committed during a public disturbance

War and warlike perils

- Insurrection, revolution and rebellion: Deliberate, organized armed citizen/ subject resistance to a sovereign government's laws
- Coup d'état; mutiny: Sudden, violent and illegal overthrow of a sovereign government; resistance by members of legally armed or peace-keeping forces to a superior officer
- War; civil war: Conflict between two or more sovereign nations, declared or undeclared; a war carried out between or among opposing citizens of the same country or nation.

References

1 Carnegie Endowment Global Protest Tracker, as of March 28, 2025

2 Allianz Research, Little fires everywhere: How polarization is shaping the economy (and what to do about it), November 18, 2024

3 VOA, Kenya grapples with protests despite political unity efforts, December 30, 2024

4 BBC, Protests erupt in Turkey after Erdogan rival arrested, March 19, 2025

5 Vision of Humanity, Global Terrorism Index 2025

6 Vision of Humanity, Global Terrorism Index 2025

7 United Nations, Secretary General's new report highlights new, emerging form of "far-right terrorism", August 3, 2022

8 Council of the EU, Sanctions against terrorism, Council renews the EU Terrorist list and designates a new entry, July 26, 2024

9 The International Centre for Counter-Terrorism, The Base, and the basis for listing far-right terror groups, July 26, 2024

10 OIET, Far-right violence and terrorism, December 2024, January 8, 2025

11 BBC, Antisemitic incidents in US surge to record high – report, October 6, 2024

12 The Parliament, Hybrid threats: Russia's shadow war escalates across Europe, January 21, 2025

13 FTM, The North Sea investigations, Almost 200 Russian ships suspected of spying in the North Sea, June 20, 2024

14 Reuters, Russia's suspected sabotage campaign steps up in Europe, October 21, 2024

15 Sky News, Counter-terror police investigate whether Russia was involved in suspicious package fire at DHL warehouse in Birmingham, October 17, 2024

16 The Telegraph, Russia suspected of trying to parcel-bomb German aircraft, October 15, 2024

17 The Guardian, North Korea behind $1.5bn hack of crypto exchange ByBit, says FBI, February 27, 2025

18 CNN, Russia-linked hacking group claims to have targeted Indiana water plant, April 22, 2024

19 BBC, Colonial hack: How did cyber-attackers shut off pipeline? May 10 2021

20 BBC, Hackers behind Ukraine power cuts, says US, February 25, 2016

21 BBC, Poland investigates cyber-attack on rail network, August 26, 2023

22 World Meteorological Organization, WMO confirms 2024 as warmest year on record at about 1.55°C above pre-industrial level, January 10, 2025

23 BBC, Trump vows to leave Paris climate agreement and 'drill, baby, drill', January 20, 2025

24 Energy Monitor, Which governments are backpedalling on climate commitments?, August 21, 2024

25 Control Risks/Seerist, Ten global topics and trends to watch in 2024

26 Reuters, Tesla says German plant power outage to continue until end of next week, March 7, 2024

27 Global Concrete, Arson attack at Cemex Deutschland's Kreuzberg concrete plant, January 2, 2024

28 The Guardian, Man arrested after climate activists cut UK insurance firms' fibre optic cables, January 24, 2025

About Allianz Commercial

Allianz Commercial is the center of expertise and global line of Allianz Group for insuring mid-sized businesses, large enterprises and specialist risks. Among our customers are the world's largest consumer brands, financial institutions and industry players, the global aviation and shipping industry as well as family-owned and medium enterprises which are the backbone of the economy. We also cover unique risks such as offshore wind parks, infrastructure projects or film productions.

Powered by the employees, financial strength, and network of the world's #1 insurance brand, as ranked by Interbrand, we work together to help our customers prepare for what's ahead: They trust us to provide a wide range of traditional and alternative risk transfer solutions, outstanding risk consulting and multinational services as well as seamless claims handling.

The trade name Allianz Commercial brings together the large corporate insurance business of Allianz Global Corporate & Specialty (AGCS) and the commercial insurance business of national Allianz Property & Casualty entities serving mid-sized companies. We are present in over 200 countries and territories either through our own teams or the Allianz Group network and partners. In 2023, the integrated business of Allianz Commercial generated around €18 billion in gross premium globally.

Further information and contacts

For more detailed information on political violence and terrorism insurance, please contact your regional Allianz Commercial contacts.

commercial.allianz.com

Email: az.commercial.communications@allianz.com

Allianz Global Corporate & Specialty SE, Königinstraße 28, 80802 Munich, Germany.

Commercial Register: Munich, HRB 208312

April 2025