RED5

# REPORT
# 2025 SECURITY TRENDS

## Geopolitical Tensions, Trade Disruptions, and Strategic Shifts


**CHIEF EDITOR** Karna McGarry

**FIRST LINE EDITOR** Michael Searway

**CONTRIBUTING AUTHORS** Omar Elshamy, Chad Kunkle, Linneu Salles, Daniel Powell, Steven Duke, Dakota Hudson, Nicholas Nemtuda and Wagner Horta

# Introduction

Like all businesses, the security industry exists on a shifting, ever-evolving landscape. Unlike other businesses, which are shaped by trends--implying "here today, gone tomorrow"--security is shaped by events that impact risk levels for individuals and organizations.

World events–changes in governments, economic tariffs, natural disasters, wars, labor strikes–create ramifications that can last for years.

This white paper focuses on events that are currently impacting the security environment in 2025 and beyond. Security professionals are tasked with assessing immediate risk, but also assessing broader threats which can impact long-term business decisions.

**For example, should you abandon a market or change your base of operations as a result of potential tariffs or economic policy changes that could be altered in the coming years?**

The impact of US economic policy is just one of many concerns that security professionals must contend with in 2025. There is also the risk of continued violence and volatility in the areas of the Middle East that threaten the supply chain, the continued war in Ukraine, and the increasing impact of natural disasters and biohazards.

# MESSAGE FROM THE CEO

As we move into 2025, the global landscape remains complex and volatile, with key geopolitical tensions and the ongoing impacts of climate change presenting significant challenges for businesses worldwide.

**KRIS COLEMAN**
FOUNDER & CEO, RED5

In this white paper, we provide an in-depth look at critical hotspots—from the Middle East to East Asia—where the potential for trade disruptions, regional instability, and even escalation into broader conflicts remains high. We also explore the growing environmental risks, including extreme weather events and shifting climate patterns, which are poised to stress infrastructure and supply chains across the globe

It is my privilege to introduce our latest white paper showcasing 2025's upcoming security trends, where our analysts explore the far-reaching impact of geopolitical tensions, trade disruptions, and strategic shifts on international business operations. This paper offers crucial insights on how these issues are likely to unfold, their potential impact on operations, and what steps we can take to mitigate these risks in the year ahead.

Our commitment to navigating these challenges for our clients is unwavering. We are actively reassessing our strategies and enhancing our risk management protocols to ensure the safety of clients and the integrity of our operations. It is crucial that we stay informed and agile in this evolving environment.

# TABLE OF CONTENTS

# ABOUT RED5

## ABOUT US

Our purpose is to ensure bad things don't happen to good people. We leverage our depth of expertise and capabilities to deliver security and risk management services that protect clients from both known and unknown threats.

The excellence of our entire team is driven by robust and diverse backgrounds across agencies, the private sector, and public sector organizations. Red5 consists of individuals who are recognized within their networks for solving problems others couldn't. We establish strong partnerships with our clients to ensure safe and successful results.

## WHAT WE DO

Red5 provides comprehensive managed service solutions for threat monitoring, privacy, and intelligence services.

We're always there to protect you, even when you don't notice. Our analysts use industry-leading intelligence tools and best practices to give you expert-led **security intelligence, threat monitoring**, and **privacy solutions**.

## 5 CORE TENETS

- **Confidentiality**
- **Authenticity**
- **Responsiveness**
- **Rigor**
- **Agility**

# THE GAZA-ISRAEL-LEBANON CONFLICT: LOW RISK OF BROADER REGIONAL EXPANSION

**These global hotspots remain areas of concern due to their impact on key transportation routes and potential for spillover of hostilities.**

The Israel-Palestine conflict will probably remain confined to Israel and its neighboring countries; while 2024 saw a rise in direct escalations between Israel and Iran, a full-scale war between both countries is unlikely in 2025.

Both Israel and Iran want to avoid a direct conflict between each other. For its part, Israel is already fighting on two fronts in Gaza and Lebanon, while Iran does not want to escalate the conflict and risk US involvement.

The removal of Bashir al-Assad and his regime provides a shift in the existing power dynamic among Syria's neighbors and foreign counties, like Russia, who were aligned with Assad's regime.

# GLOBAL HOTSPOTS - GAZA-ISREAL-LEBANON CONFLICT

The Israel-Palestine conflict has negatively affected corporations and supply chains linked to the Middle East since late 2023, and has intensified due to the conflict's limited expansion towards Lebanon and the Red Sea.

Iranian proxies such as the Houthis and Hezbollah will likely continue to attack commercial vessels in the Red Sea and near the Bab-el-Mandeb Strait.

- Cargo volume for the Suez Canal fell 62% in the first half of 2024, and insurance costs for vessels passing through the Red Sea have nearly doubled; companies involved in trade throughout the Red Sea will likely continue to face such trends in 2025.

- Corporations with a presence in conflicted areas should thus continue to expect both business disruptions and physical security risks.

If the conflict expands to involve Iran, then Gulf countries would see an increase in attacks on shipping routes and oil refineries. The impact of this would be increased oil and gas prices worldwide.

Diplomatic efforts by the US and Persian Gulf states, such as Saudi Arabia and the United Arab Emirates, can serve as a mitigating factor as long as Israel limits its attacks against Iran to military targets, and avoids nuclear facilities or oil refineries.



# THE TAIWAN STRAIT: HIGH TENSIONS, NO IMMEDIATE RISK OF ESCALATION

**There is no strong evidence that China is preparing for a full invasion or blockade of Taiwan in 2025, but the risk for continued escalations remains high.**

Corporations involved in trade across East Asia will need to maintain a high level of readiness for potential business disruptions.

China has continued to increase military provocation in the strait, with PLA (People's Liberation Army) air incursions rising from 36 in January 2024 to 193 in August of the same year.

# TENSIONS IN EAST ASIA - THE TAIWAN STRAIT


**In 2022 alone, nearly $586 billion worth of trade has traveled through the Taiwan Strait, with one-third of global shipping passing through the South China Sea.**

Sustained actions from the PLA have further normalized a Chinese presence around Taiwan, indicating their intent to invade and annex the island–an explicit goal of the Chinese Communist Party.

A blockade or invasion would likely cause significant disruption to global trade, particularly given the size of the island's microchip processor industry, which is critical for the development of consumer goods, military hardware, and artificial intelligence.

The US government and private sector experts have suggested that an escalated conflict in 2025 is unlikely, instead pointing to the PLA centenary in 2027 as a more concerning date.

The Chinese military, however, has an interest in maintaining secretive invasion plans, which complicates efforts at forecasting their intent or timeline.



# THE KOREAS: NEW INSTABILITY CAUSED BY MARTIAL LAW

**The declaration of martial law on 3 December 2024 by South Korean president Yoon Suk Yeol, despite only lasting for several hours, has set the stage for a possible change in national leadership following his impeachment.**

The follow-on impact could be a significant change in South Korean international policy.

The martial law order followed months of political turmoil for President Yoon, and his impeachment has raised the possibility that new presidential elections will be held in South Korea in 2025.

Different election outcomes are possible, which would likely prove highly consequential for South Korea's relationship with the international community.

**For example:**

- If Yoon is declared innocent, or if his People's Power Party (PPP) wins in a reelection, then South Korea's policy regarding North Korea, the US, and Japan would remain the same.

- If the Democratic Party wins in an election, then South Korea's policy is almost certain to shift towards a more conciliatory relation with North Korea and China, while being more cautious towards a relationship with Japan.

Red5 intelligence analysts find that there is no immediate risk for an armed conflict against North Korea in 2025, regardless of the ongoing political instability and election prospects in South Korea.

Although President Yoon's decision to implement martial law has been vetoed, it still could be seen by North Korea as an opportunity for escalation and provocation to undermine re-established order. North Korea could push disinformation to subvert any efforts to restore political and social order in South Korea.

## Ukraine: Limited Change

Neither Ukrainian nor Russian principal strategic objectives have been achieved, but the Trump administration has explicitly stated it wants the war to end.

European countries have expressed continued support of Ukraine through 2025, and the US will likely continue to both assist Ukraine and attempt to avoid further escalations.

Land fortifications and low weapon stockpiles have stabilized battlefield lines, meaning offensive operations are unlikely to significantly change territorial control in 2025.



# INTERNATIONAL DIPLOMACY

**Changes in government leadership in the US, Canada, and Mexico will bring change to foreign policy and trade that will have second-order effects on business operations.**

US diplomacy will likely shift to a more confrontational and transactional approach in 2025 with the incoming administration. President Donald Trump's return to the White House will likely affect US-based corporations, including economic policy changes that will impact corporations' overseas operations.

One of the most consequential changes may be felt in the relationship with China, although US rapport with other countries in East Asia and Europe will also be altered, especially as several face serious domestic political turmoil and may pursue interests at odds with those of the United States.

Changes to US economic policy in the areas of trade and tariffs will certainly impact existing diplomatic relationships, even amongst US allies.

In early 2023, China passed an amendment to a law designed to protect against foreign espionage, which gives the government stronger controls over data collection and an increased ability to criminalize what were once considered normal business activities.

This raised concerns by US businesses that Chinese officials could arbitrarily enforce such laws to punish companies, especially after CCP officials indicated that the law may be enforced in response to comments and official stances by companies that run counter to China's national interests.

Soon after this law was passed, Chinese law enforcement raided the offices for US based companies, detained several employees, and placed exit bans on executives.

See, “Beyond the Great Firewall” for a more in-depth discussion of China’s role in espionage, cyber and IP threats, and international business operations.

The atmosphere has changed after China released three detained US citizens as part of a prisoner swap and the US State Department lowered its advisory rating. China will continue to use this as a tool at its disposal in response to any negative actions by the US government.

The risk of capricious detainment and exit bans from China may escalate in response to the Trump administration's anticipated tariffs on Chinese products. China has adjusted laws designed to punish companies that adhere to sanctions placed on China.

It has developed a procedure to open investigations into "unreliable entities" that are perceived to be at odds with Chinese business practices and interests such as statements on issues including Taiwan and Tik Tok. A probe was opened on the PVH Group in September 2024 for allegedly interfering in the supply chain for China's Xinjiang province, which has been subject to international sanctions related to allegations of forced labor.

US corporations will continue to have to adjust their business operations should the Trump administration follow through with its stated intentions to take a tougher stance against China.



# INTERNATIONAL TRADE

**Companies are already preparing for changes in economic policy, which vary in impact but will require companies to assess business operations within new security environments.**

President Trump has demonstrated his willingness to deploy tariffs, both as a means to rebalance U.S. trade deficits and as leverage for other foreign policy goals.

The practice of near shoring could increase and present security officials with new security landscapes to assess risk, in the immediate and long term.

Changes in the operating environment require assessing transportation, workforce capabilities, crime, natural disasters, political, and economic stability.

This may prompt security teams who are currently focused on a particular geographical area to pivot to a completely new region and different problem set. Businesses need to plan for reassessing new security landscapes if economic policies necessitate a change of physical infrastructure

**Universal tariffs may make trade with the European Union (EU) more expensive.**

- The United States currently maintains a $230 billion trade deficit with the EU, and President Trump has previously expressed dissatisfaction with EU tariffs being higher than their US equivalents, particularly in the automotive and agricultural industries.
- His proposed 10% to 20% universal increase could result in European nations attempting to shift a portion of their trade to other allied nations, and engage in retaliatory responses to US tariffs.

**The Trump administration will likely attempt to alter the United States-Mexico-Canada Agreement (USMCA) to find better terms for US businesses, particularly in the automotive and agricultural industries.**

- The USMCA renegotiation is scheduled for 2026, but the Trump administration will seek to even trade deficits with tariffs.
- President Trump has declared a 25% tariff on all imports from Canada and Mexico unless both countries halt the flow of illegal drugs and immigration.
- Given that the United States imported nearly $900 billion worth of goods from Canada and Mexico in 2022, such a measure could result in significant price increases if both countries were to engage in retaliatory actions.

**Similarly, President Trump has mentioned the possibility of an additional 10% blanket tariff on all Chinese imports if the PRC does not disrupt the flow of fentanyl into the United States.**

- During his election campaign, Trump threatened tariffs of up to 60% against Chinese imports.
- China has leverage to institute its own damaging sanctions–it is the United States' largest trading partner with over $750 billion in bilateral trade, and moreover has reduced its dependency on US goods and services since the first Trump administration.

In addition to general tariffs on trade, the United States and China are engaged in an increasingly volatile tech trade war. Following US restrictions on technology sales to China, particularly advanced semiconductor products, the PRC responded with restrictions on exports of certain goods used in military and high tech purposes.

Most recently, China outright banned the sale of specific rare earth minerals to the United States. Continued escalation of this tech trade war not only has the potential to limit economic growth, but to also significantly constrain US supply chains, particularly in Chinese-dominated areas such as rare earth minerals.



# CLIMATE CHANGE IN THE US: EXTREME CLIMATES STRESS DOMESTIC INFRASTRUCTURE, REQUIRE REVISED EMERGENCY PLANS

**The continued risk of natural disasters and biohazards requires corporations to keep their business continuity plans and emergency action plans as living documents.**

The start of 2025 in the US has already experienced devastating wildfires in California and winter storms in parts of the country not prepared for ice and snow.

Natural disasters will damage existing infrastructure as most US bridges, roads, and railways are aging and remain vulnerable to severe weather events.

## IMPACTS ON CORPORATIONS - WEATHER EFFECTS ON FUTURE PANDEMICS

Increased heat waves and high winds will strain US energy critical infrastructure and decrease productivity for corporations. The Federal Emergency Management Administration (FEMA) introduced climate adaptation planning to foster climate resilience in the workplace in 2024, stressing the importance of climate impacts to businesses and communities.

Increases in environmental risks will stress conventional emergency action plans that are often too generic and lack sufficient training and preparation.

**La Niña will likely cause more extreme weather events in the United States that will stress transportation and logistics networks in 2025.**

The National Oceanic and Atmospheric Administration (NOAA) and the United Nations Climate Report predict a strong La Niña to increase heavy rain in the northern United States and create a warmer southern region in 2025.

This change in weather patterns will lead to increased drought conditions in the Sun Belt for 2025 and will increase the chances of blizzards and flooding in the Northeast.

The United States could lose billions of dollars due to more intense storms, destruction of infrastructure, and production and logistical delays. Billion-dollar weather events in the US have increased from roughly every four months to every three weeks since 1980. Weather was the cause of 23% of all road delays in the United States in 2024, which costs transportation companies $2 to $3 billion annually.

Companies will need to invest in increasing inventory levels, reorganizing supply chain bases, and upgrading infrastructure to remain connected in the event of severe weather incidents.



# CLIMATE IMPACTS ON FUTURE PANDEMICS: CHALLENGES AND OPPORTUNITIES FOR CORPORATIONS

**Corporations should increase their vigilance and monitoring to combat future pandemics in 2025.**

Corporations should avoid relying solely on health data released by local agencies or government bodies, because they are often released after there is already an issue.

Chief security officers tasked with monitoring global workforce and supply chains will need to create their own data collection systems to ensure there is an early warning that provides them with the lead time to make business decisions instead of reacting to an event.

## IMPACTS ON CORPORATIONS - WEATHER EFFECTS ON FUTURE PANDEMICS

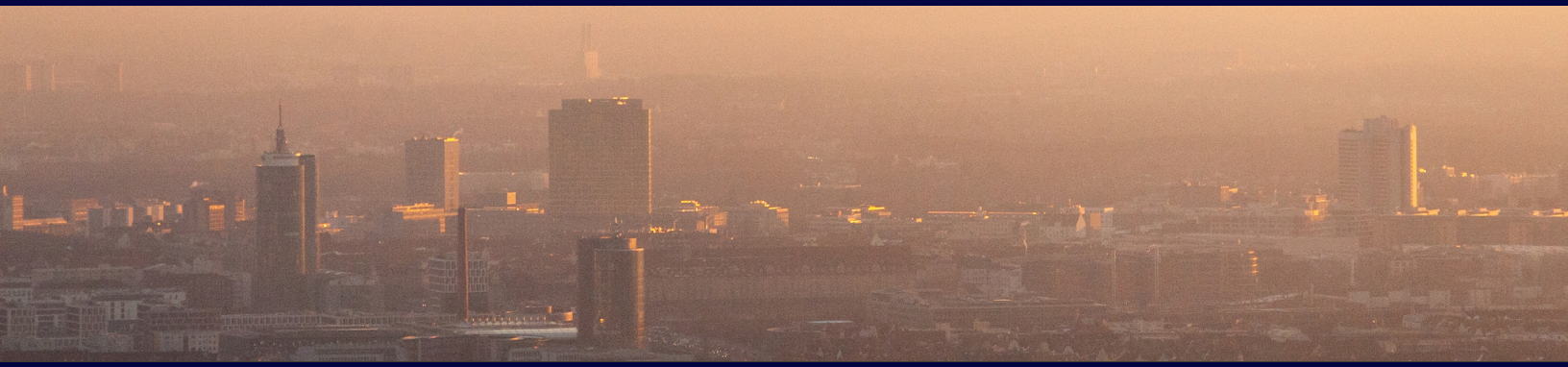
The reality is that biohazards, whether natural or manmade, should be considered in a company's risk matrix instead of being viewed as a black swan event.

Corporations should invest in communications, advanced warning, and health services to detect workforce outages across their corporate structure; with global footprints, multi-national corporations can have global insight into potential outbreaks before they grow out of control.

The average global temperature in 2024 was the highest on record and one risk of the increase in temperatures is a shift in the natural range of previous pathogens into differing geographic areas at different times of the year.

- For example, the increase in precipitation and warmer climates will likely spread the range of habitability for mosquito-carried diseases.
- The UNDP predicts a 20% increase in cases of cholera, Zika virus, and chikungunya virus infections due to rising temperatures.

The World Health Organization (WHO) will conclude their international pandemic preparedness treaty in 2025, which will lay the groundwork for contingency plans for future outbreaks.





# REPUTATIONAL AND CYBER THREAT LANDSCAPE FOR CORPORATIONS

**Companies that are perceived to support certain social or political causes will continue to face increased risks of reputational harm from activists in 2025.**

The public perception that corporate actions are in support of a social or political cause will continue to increase.

Corporations will face public scrutiny on both direct business agreements with controversial actors and indirect financial relationships.

This practice is becoming increasingly common among online activists, aided by social media and the availability of public business and financial records.

# IMPACTS ON CORPORATIONS - REPUTATIONAL/CYBER THREATS

- **Reputational damage via social media spreads quickly and is often unchecked, drawing the attention of activists calling for boycotts or protests, which has intensified with the spread of AI-based misinformation (see below).**
- **Risk associated with insider threats may also increase, should employees become disgruntled with the perceived beliefs or actions taken by their employer.**
- **Growing international tensions will create additional avenues for companies to be targeted by activists, due to their involvement (perceived or real) in various diplomatic or kinetic conflicts.**

Actions taken by a company and its leadership team – whether they are acting on behalf of the company or not – directly impact the risk of targeted reputational or physical harm. Official statements and social media activity are well-known avenues by which a company or executive can incur reputational harm.

There are, however, additional sources online activists can utilize to identify targets, such as voter registration and political contribution records, both of which are publicly available to varying degrees based on local and state regulation.



# ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: INCREASINGLY SOPHISTICATED ATTACKS

**The frequency and sophistication of AI-powered attacks will likely increase in the coming year due to the increasing adoption of AI tools by various threat actors, which will pose novel and complex risks for reputational harm.**

The initial period of exploration and gradual adoption of AI technologies by threat actors seen in the last several years is ending, giving way to an era where AI tools are widely used to perpetrate attacks.

This is fueled by the rapid evolution of AI technologies and the increasing ease with which they can be adopted.

As threat actors experiment with new AI tools, the sophistication of attacks will continuously increase and be employed in varied ways, including tarnishing companies' reputation, social engineering, and mounting malware campaigns.

# IMPACTS ON CORPORATIONS - AI AND CYBERSECURITY

**While AI will increase the severity and frequency of cyberattacks, threat actors will likely continue to use the same tactics.**

- Threat actors will continue to use social engineering tactics to fool targets, but will also utilize AI to create significantly more convincing deepfakes and digital messages.
- Malware campaigns have also been empowered by AI: large language models can assist threat actors with little coding experience to write computer viruses, reducing the time and resources needed to deploy them.

**The widespread adoption of AI technologies have qualitatively changed reputational harm risks for companies.**

- AI-based impersonation is a particularly concerning avenue for reputational harm that companies need to preemptively address, as mechanisms for identifying whether content is AI-generated are still nascent and not always reliable.
- AI tools enable threat actors to convincingly impersonate company officials in order to spread false information, either as a way to target a company's own reputation or propagate false narratives.

## IMPACTS ON CORPORATIONS - AI AND CYBERSECURITY

Some social media platforms, like Facebook and YouTube, have adopted preliminary mechanisms for automatically detecting AI-generated images, but there are ways to circumvent these and it remains difficult to detect video or audio deepfakes.

**2025 will likely see a significant increase in AI-based reputational attacks, as threat actors will seek to spread propaganda and sow civil unrest domestically and internationally.**

Companies will need to actively monitor online discourse about them and preemptively seek to counter false narratives with their own information campaigns. Defamatory AI-generated content is currently able to propagate online with few obstacles, particularly if threat actors have spent significant time refining them to be believable.

AI developing companies, social media platforms, and policymakers have not established widely-accepted systems for flagging AI content - and even if they eventually do, not all online spaces will necessarily adopt them.

This has created a significantly higher risk of reputational harm for companies, particularly if they are involved in controversial issues or are targeted by actors with the resources for extensively refining AI content, such as state-sponsored groups or wealthy industry competitors.

Organizations should also consider whether mechanisms protecting customers are necessary, as instances where company representatives are impersonated via AI may create situations of corporate liability.

# Outlook

Security professionals in 2025 will face a similar array of challenges that is posed every year. However, the changes in the US administration, ongoing global hotspots, and the recent events that have highlighted the individualized risk to C-suite will require leadership to prioritize personnel and budget to address these risks.

There are some areas of overlap, but not enough to allow security–which is typically a cost center–to provide adequate resources to address all the challenges equally.

For example, security professionals are often charged with both assessing risk for an enterprise and meeting the immediate tactical needs of their C-suite and other business leaders, all within the context of their individualized threat landscape.

In addition to executive protection for leadership, recent events underscored the need for companies to invest in internal risk assessment, such as insider threats and workplace violence.

The risk to leadership garners press attention, but the risk to employees by fellow employees or personal connections is a more common occurrence and poses a significant risk to a company's workforce.

# How Red5 Can Help

***Escalating global security trends highlight the need for corporations to be well-informed of the unique threats they face, which are multiplying in an increasingly uncertain and unstable world.***

Red5 analysts leverage their in-house expertise to proactively monitor the global threat space to remain well-informed, decipher ambiguous security challenges, and produce tailored and actionable security solutions for our clients. Our analysts use industry-leading intelligence tools and best practices to give you expert-led managed security intelligence, threat monitoring, and privacy solutions.

**Managed Intelligence & Analysis**

- Expert-led monitoring, analysis, and insights
- Flexible investigations and reports, adaptable to changing needs and risks
- Monitor for threats across mainstream and alternative social media

**Managed Threat Monitoring**

- Remove fake or impersonation accounts
- Dark web surveillance for compromised credentials
- Geofenced monitoring of location-specific threats

**Managed Privacy Solutions**

- Understand the full-picture of your digital footprint and how to minimize risks
- Remove your personal information as quickly as its bought, sold, and shared with WebScrub
- Protect against common attack tactics, hacking attempts, scams, and spam

## GET IN TOUCH TO LEARN MORE

 red5security.com/contact-us

 info@red5security.com