SPS Global Insights

The Importance of Geopolitics to Business

This report addresses the crucial link between geopolitical events and business implications, highlighting risks like supply chain disruptions, political instability, and cybercrime as the real world impact of mounting global tensions.

Introduction

As an intelligence analyst focussing on geopolitics, clients often ask... "Why is this important to me?". "What are the implications?" Translating at times seemingly abstract geopolitical phenomena into business implications is essential to the role. At SPS, we understand the ramifications of political instability through past cases leading to the need for political awareness, and we aim to keep our clients one step ahead of global events. In this report, we outline the reason why political instability and geopolitical tensions remain so pivotal to today's and tomorrow's security landscape. From political coups driving an increase in terrorism and domestic unrest, state-sponsored actions of cybercrime, to increasing reputational and financial losses, global political dynamics continue to impact businesses' profits and employees' personal safety. In this report, we outline five key risks SPS believes highlight the significant need for geopolitical awareness including: supply chain disruptions, political instability, conflict and violence, regulatory uncertainty, and state-sponsored cybercrime. Late reactions and outdated just-in-time security responses can not only lead to severe financial losses but also heightened safety concerns. Therefore, in an increasingly volatile world, maintaining not only situational awareness, but also an ability to forecast future risks through deeper geopolitical context promises to deliver industry-leading security and greater financial profitability.

Recent Examples of Geopolitical Impact

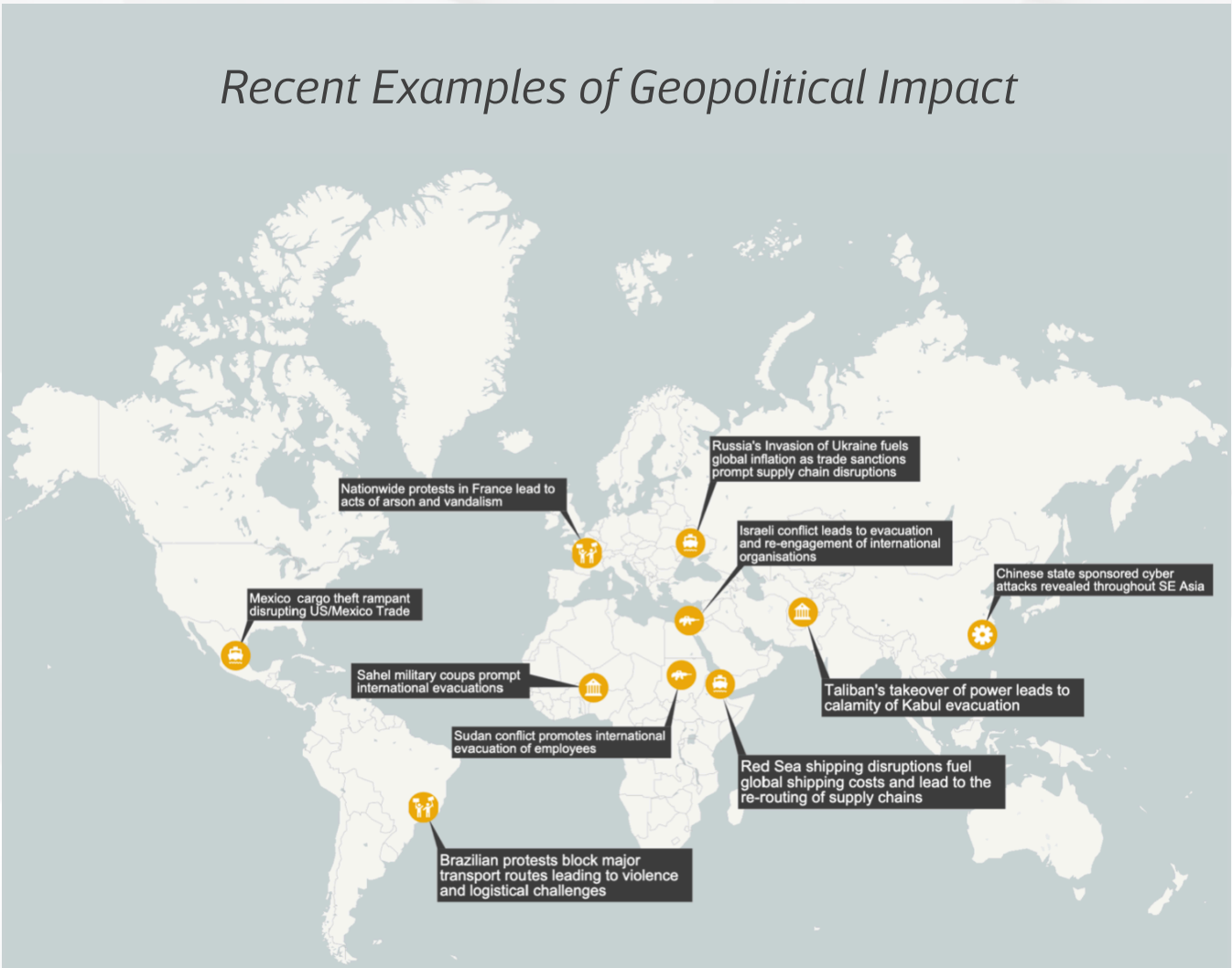
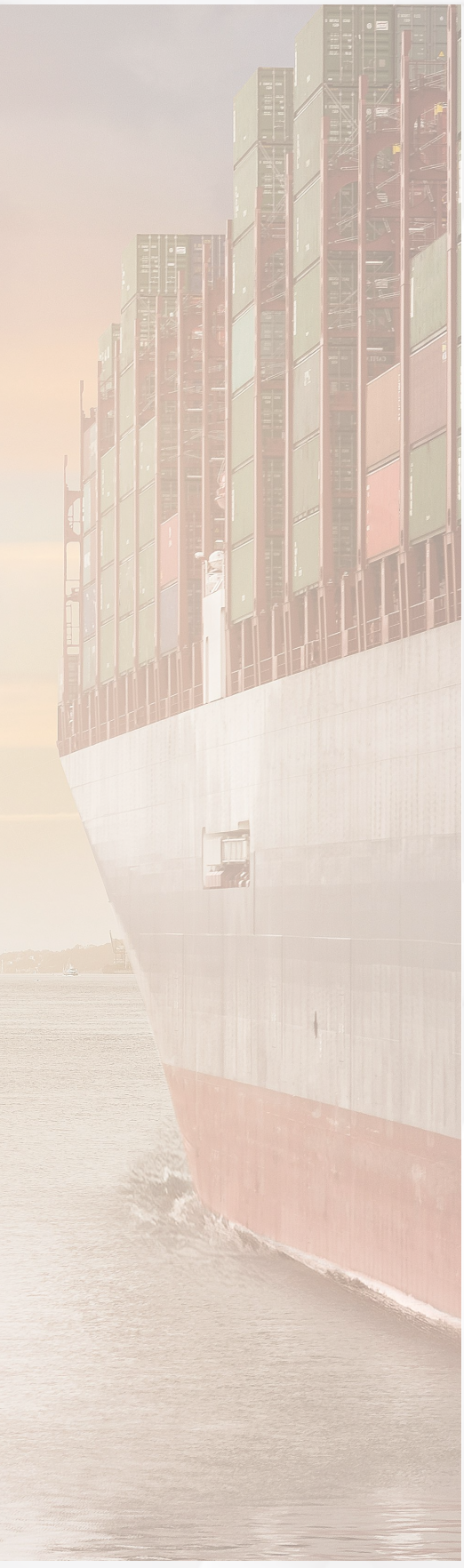


Figure 1: Geopolitical Case Studies

Supply Chain Disruptions

In the aftermath of the Covid-19 pandemic, multinational corporations are addressing vulnerabilities in global supply chains. The once-clear distinction between domestic and foreign production has long been blurred by globalisation, requiring businesses to maintain global awareness of risks. The ability for global conflict and tension to disrupt international business was seen in Ukraine and now more recently in the disrupted supply chains of the Red Sea. The impacts of such events are felt globally, as indicated by a recent survey from the British Chamber of Commerce, which showed that 55% of UK exporters are grappling with elevated shipping costs and delays. The emergence of drone technology has empowered non-state actors, such as the Houthi rebels, to disrupt international cargo, impacting insurance and global supply networks. War risk premiums for Red Sea voyages have surged to around 1% of a ship's value (up from 0.7%) contributing to global inflationary pressures.



Aside from direct conflict, geopolitical tensions, like those between the US and China illustrated by Section 301 tariffs, have fuelled a rise in global protectionism and significant economic shifts. The scale of disruptions and relocations of supply due to such geopolitical tensions should not be underestimated. This was highlighted in a recent trade analysis by Tori Smith and Tom Lee at the American Action Forum which showed that the cost to US consumers has collectively reached +$48 billion. Notably, half of this amount was shouldered by US firms, highlighting the drastic financial impacts that geopolitical tensions can have on global supply chains and profit margins. Such events have prompted an increase in nearshoring, with businesses seeking proximity to consumer bases to mitigate disruptions. However, even locations such as Mexico or Eastern Europe present challenges involving instability and armed conflict, imposing additional costs on businesses. In Mexico, for example, annual losses from cargo theft have been estimated by the Association of National Transporters at over 2.3 billion pesos, as violent incidents increasingly necessitate additional security needs and global assistance even in businesses' near abroad.

As global tensions intensify, the targeting of supply chains remains a potent tool for non-state actors. Businesses are compelled to invest in protective security measures and adaptable supply chain risk management strategies to navigate an increasingly challenging landscape. In this fragmented world order, a crucial aspect for strategically positioning workplaces and ensuring business resilience stems from an understanding of bilateral relations and the future direction of geopolitics.

Conflict and Violence

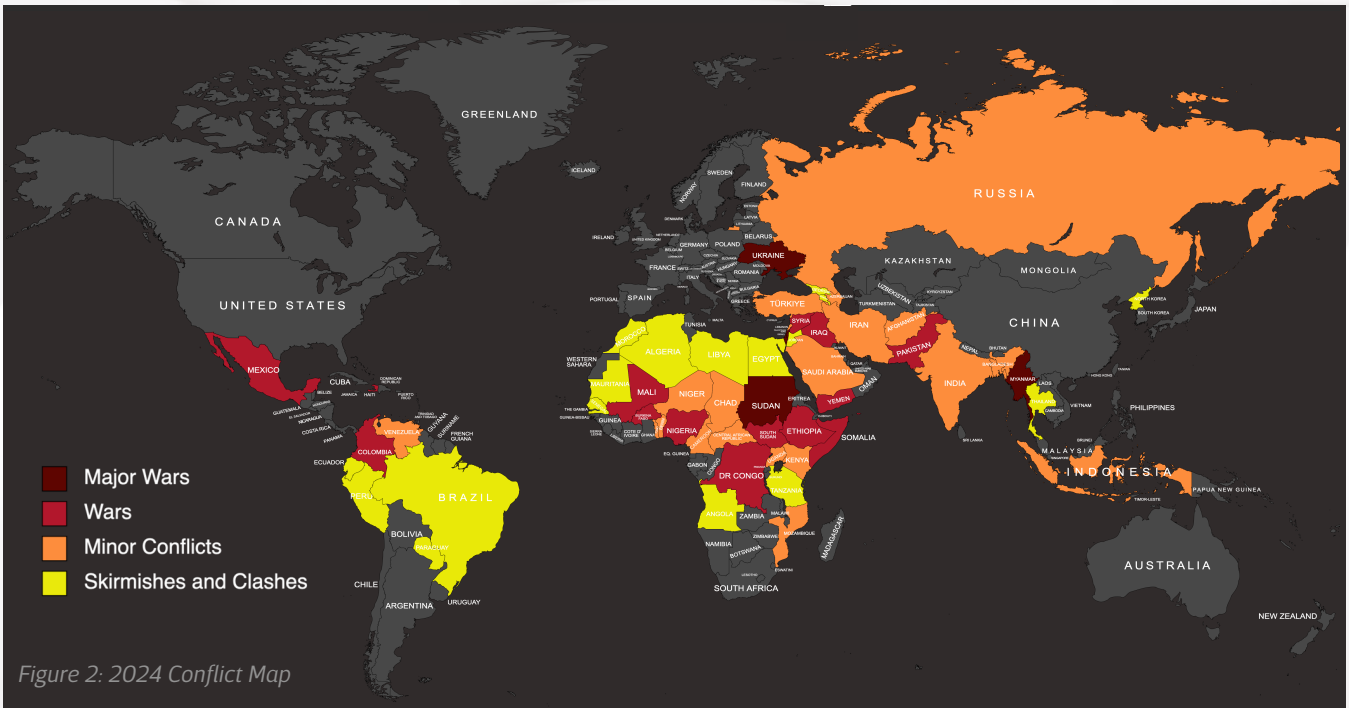


Figure 2: 2024 Conflict Map

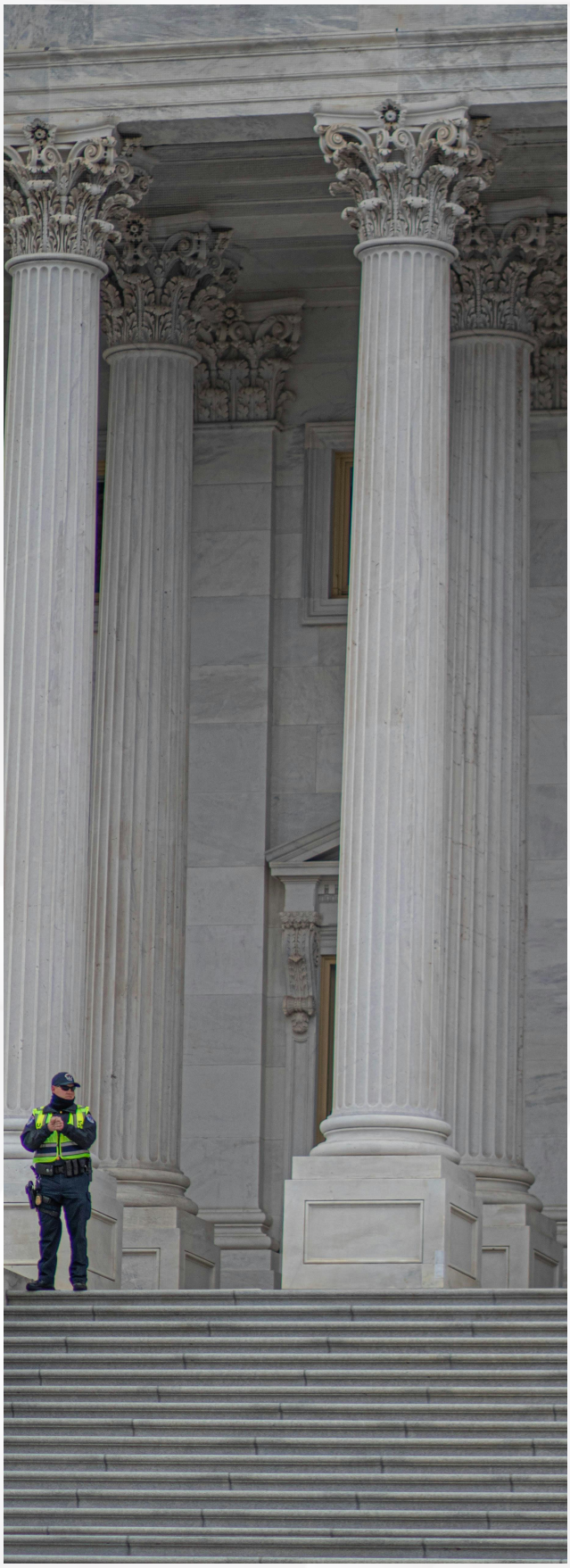
The increasing volatility of the world continues to contribute to the persistence and eruption of conflict and violence, which profoundly affect global businesses by posing significant challenges to their operations, sustainability, and growth. One in six people now live in conflict areas, resulting in global risks for businesses, especially as conflict zones coincide with crucial trade routes and resource-rich regions. This leads to increased costs, delays, and uncertainty for companies and employees. Violence can directly harm businesses, resulting in physical damage and asset loss, deterring investments and impeding development. Furthermore, businesses in conflict-prone areas may struggle to safeguard, attract, and retain skilled workers due to safety concerns which must be mitigated by proactive security measures. Therefore, understanding the trajectory of ongoing conflicts including potential future scenarios remains critical for the global operation of businesses. The Armed Conflict and Event Data Project has reported a 22% increase in incidents of political violence, resulting in at least 167,800 fatalities through 2023, highlighting the increasing volatility of today's world.

Additionally, the prevalence of conflict creates a challenging regulatory environment, with governments imposing restrictions and emergency measures that impact business operations, increasing financial risks and hindering strategic planning. The long-term consequences can be profound, as businesses in conflict areas face challenges in rebuilding trust and reputation, even after a conflict's resolution. Last-minute international evacuations are often chaotic and expensive. Forecasting future areas of conflict through a deep understanding of the rising tensions of nations is therefore not only an essential security measure to safeguard business assets and personnel, but can also deliver reduced crisis response costs.

We also observe the changing dynamics of conflicts. Modern precision weaponry promised an era of lower civilian fatalities; in spite of this, the continuing scourge of terrorism and non-state actor violence, who frequently rely on less technologically advanced and more indiscriminately harmful tactics, continues to contribute personal safety risks to employees in high-risk areas. An understanding of the tactics, security mitigations and disaster plans are now more pivotal than ever in safeguarding areas of heightened risk which can only be forged with a deep understanding of the risk of conflict and violence in any given location.

Regulatory Uncertainty

Ongoing geopolitical tensions remain deeply tied to national regulatory environments and changes global business operations face. Across many nations the surge in autocratic leadership and military diktats has resulted in repressive legislation and a shrinking of the civic and business space. Changes in tariffs, security measures, and business practices are just some direct consequences of the evolving global compliance landscape which shadows geopolitical tensions. The expulsion of foreign security providers and international coalitions represents a particularly destabilising example, leaving business operations vulnerable in regions like the Sahel.



Moreover, tensions and international hostilities can create an unfriendly environment for foreign national companies and personnel. In China, for instance, raids on US firms and employee detentions through 2023 have reduced inward investment and posed new concerns for businesses in the region. Coupled with this, the ongoing development of new digital compliances and legislation is ever reshaping firms' cyber policies and undermining intellectual property rights.

These regulatory challenges don't just arise from autocratic measures; they can also result from liberal climate regulations. The push for net zero emissions in European countries, with a recently announced target of a 90% reduction in emissions by 2040, will necessitate significant regulatory changes impacting businesses over the coming decades. Recognising that regulatory changes stem from both progressive and regressive political changes is essential. Staying ahead of the competition and legislative landscape will enable firms to engage in better strategic planning and investments, ensuring the continuity of future operations.

As the world moves towards multipolarity, the global legislative landscape is expected to become more fragmented and impactful. Local customs and laws will increasingly vary, necessitating effective adaptations to work practices and risk evaluations for companies with global operations. To navigate this increasing fragmentation, understanding, monitoring, and forecasting regulatory risks are crucial for future profitability and sustained global operations.

Political Instability

A growing concern arises from the decline in global democracy over the past 17 years, as reported by Freedom House. This decline has most poignantly led to the emergence of military dictators, particularly in Africa, but also drives challenges to political establishments globally inclusive of Europe and America. Such instability is manifested through protests, industrial actions, elevated crime rates, and incidents of civil unrest. For example, the 2023 summer riots in France were estimated to cost the country over 1 billion euros. Analysing the political direction of nations is therefore increasingly essential for predicting future domestic unrest, military coups, and civil disturbances.

These challenges are impacting democracies worldwide. They not only contribute to financial market instability but also result in physical property damage and pose risks to employee safety. The global Protest Tracker by the Carnegie Endowment for International Peace notes that more than 132 countries have experienced major disruptive protests since 2017, underscoring the global nature of this phenomenon. As democracy faces increased challenges globally, we anticipate a rise not only in military coups but also in violent and disruptive protests, potentially leading to deadly incidents and harm to individuals. Understanding electoral cycles and domestic political developments in nations of operation is now crucial for maintaining the security and safety of facilities and employees. The frequency and severity of events of political instability and unrest are on the rise as undemocratic actions increasingly prompt disruptive major demonstrations and incidents of violence. Such demonstrations and instability also often lead to a surge in crime, such as vandalism, looting and arson, which can affect business assets.

Globally, incidents of civil unrest are reported on a near-weekly basis due to increasing political division and instability. The fragmentation of global politics, partly driven by the rise of social media, has created a more hostile political climate which does not sit separate from the workplace. We have witnessed divisive national political debates lead to incidents of workplace violence amongst employees and the need for better Human Resources and security collaboration. Even nations traditionally known for stability are not immune from these developments. Businesses must now plan more effectively for events arising from domestic political instability, starting with a comprehensive understanding of the emotional and legislative climate of nations. Effective analysis allows for the prediction of areas of concern and enables the implementation of effective security measures and employee safety protocols, positioning businesses in a stronger position to respond to the rising challenge of political unrest.

State Sponsored Cybercrime

Finally, in an increasingly fragmented world, actions of state-sponsored cybercrime continue to drive record-breaking financial losses and long-lasting reputational risks. Cyber attacks can cause significant economic and physical damage, disrupt critical services, compromise the integrity of information systems, and violate the privacy and security of individuals. Such attacks are increasingly utilised as a tool of modern warfare and target companies that reside within geopolitical adversaries. Cybercrime already results in global losses beyond the individual size of almost all national economies. Cybersecurity Ventures expects global cybercrime costs to grow over the next five years, reaching $10.5 trillion USD annually by 2025. Such estimates were made in the absence of an increasing understanding of the potential risks of artificial intelligence in developing new forms of cybercrime.

The use of cybercrime and cyber attacks by malign state or state-sponsored actors has increasingly become apparent in recent years and reflects the deepening security risks in the digital world. Such events impact even the most technologically advanced firms, as was seen in November 2023 when Microsoft announced that Russian hackers had broken into its corporate systems. Hackers used a “password spray attack” to steal emails and documents from the accounts of Microsoft’s senior leadership, cybersecurity, and legal teams. Effective cybersecurity defences can help safeguard businesses from immediate attacks. However, a better understanding of the actions of malign states and the geopolitical objectives and aims of nations such as Russia allows firms to prepare long-term defences and forecast areas of future risk through ensuring investment to counter growing trends and areas likely prone to state sponsored cyber incursions.

Geopolitical tensions only amplify cybercrime's impact on businesses, as nation-states exploit digital vulnerabilities for economic and strategic gain. State-sponsored hackers target corporate networks, aiming to steal sensitive data, disrupt operations, or undermine rivals. The blurred lines between political and cyber conflicts intensify the threat landscape, exposing organisations to sophisticated attacks with broader consequences including long-term reputational harm. The weaponisation of information and technology in geopolitical rivalries heightens the risk of collateral damage for businesses caught in the crossfire. As nations engage in cyber-espionage and warfare, companies face escalating challenges in safeguarding their assets, emphasising the critical need for robust cybersecurity measures in this era of geopolitical uncertainty.

Conclusion

This report underscores the critical connections between geopolitical tensions and the operations of global businesses, emphasising the imperative for proactive forecasting and understanding of geopolitical developments. The identified risks, encompassing supply chain disruptions, political instability, conflict and violence, regulatory uncertainty, and state-sponsored cybercrime, underscore some of the real world intricate challenges corporations face in today's geopolitically uncertain environment. Yet, despite an abundance of information, the lack of effective analysis and scrutiny can lead to heightened risks of misinterpretation.

In an increasingly volatile world, the ability to anticipate and adapt to geopolitical shifts is vital for financial stability and employee safety. Recognising the impact of political dynamics on the security landscape provides a strategic advantage, positioning businesses ahead of potential crises. Examining historical cases and current geopolitical phenomena highlights the substantial consequences at stake. Delayed responses and outdated strategies can result in financial losses and heightened safety concerns for employees. Thus, prioritising industry-leading security through continuous situational awareness and intelligence input is increasingly becoming a strategic necessity for effective business operations.

By investing in global monitoring, intelligence and security packages, curated by experienced providers, businesses can gain a nuanced understanding of evolving risks worldwide. Adopting a proactive approach facilitates the development of mitigation strategies that safeguard assets, staff, and lives. As nation-states continue to shape global security dynamics, ongoing monitoring and understanding of the fragmented global structure and foreign policy of states is essential for forward planning. Significant security incidents, whether they be an armed conflict or a wave of industrial action, tend to have precursors. Through effective analysis, intelligence providers can highlight areas of heightened concern and forecast these future developments. The sometimes seemingly abstract developments often network to show areas of future vulnerability, allowing one to secure future operations and ensure resilience in the face of evolving security challenges.

The Three Stages of Business and Travel Safety

1

Understanding

Provide knowledge to not only identify risks to both assets and personnel, but provide actionable intelligence

2

Planning

Utilisation of actionable intelligence by operational experts to assist in contingency planning and preparation

3

Assurance

24/7 monitoring and response, knowing we are reassuringly there

Contact

For more information on our services,
Please contact our Intelligence Research Team
irt@sps-global.com

This report was edited by: Oliver Maund, Lead Intelligence Analyst

Based in the Global Response Centre in Hereford, Oliver Maund is SPS's Lead Intelligence Analyst. Before joining SPS, he achieved a first-class honours degree in a joint Politics and Economics bachelor's program from Exeter University.