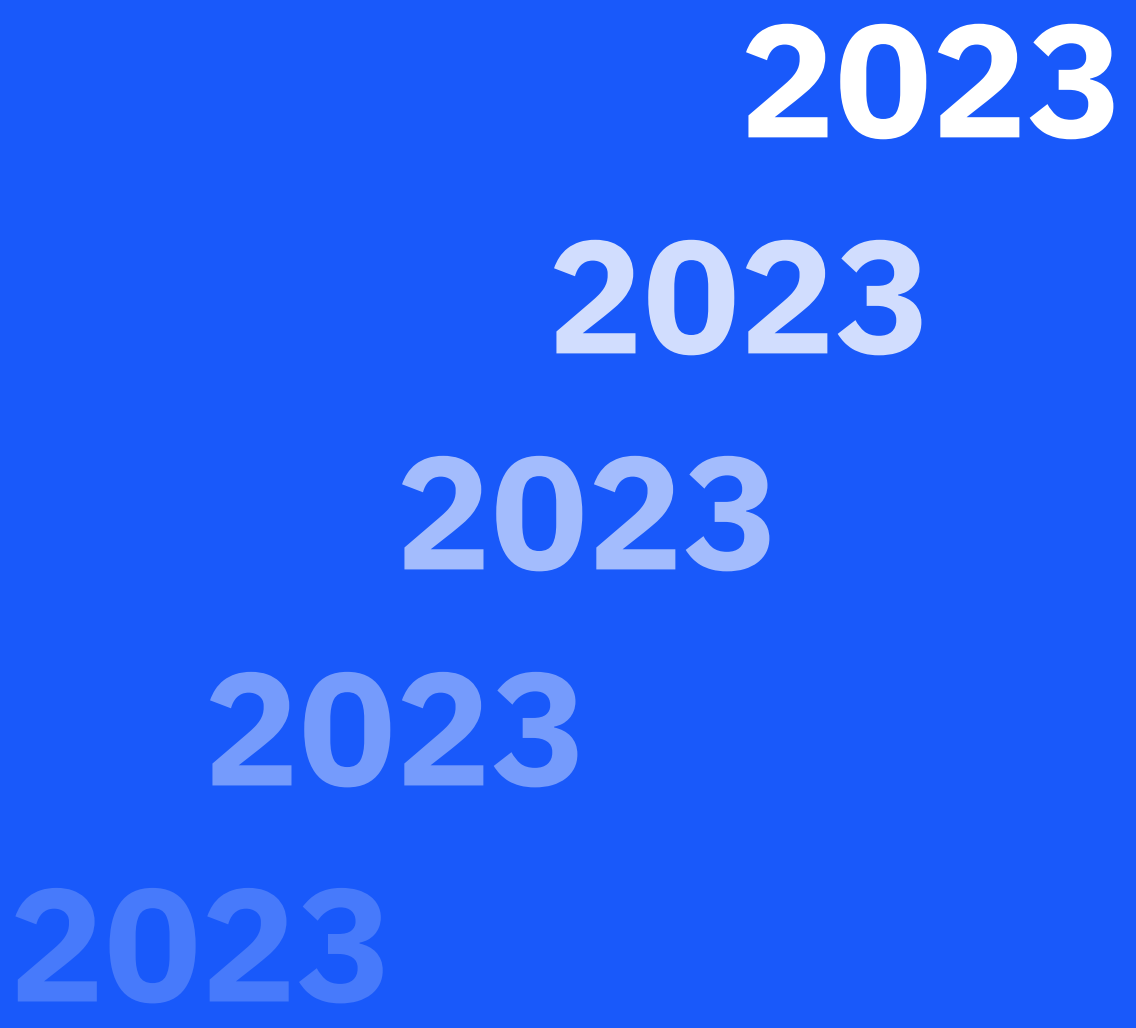


Global Risk Outlook

January, 2023

NSSG®

DISCLAIMER

While we have made every attempt to ensure that the information contained in this document has been obtained from reliable sources, the author is not responsible for the results obtained from the use of this information. In no event would the author, its related partnerships or corporations, or the partners, agent or employees therefore be liable to you or anyone else for any decision made or action taken in reliance to the information in this document.

PHOTO DISCLAIMER

All photos displayed are under the copyright licence of the Shutterstock and Unsplash platforms, as well as, NASA imagery. Special image credit of NASA, “Blue Marble-Image of the Earth from Apollo 17”.

Risk Clusters

The NSSG Intelligence Team releases its 2023 Global Risk Outlook.

This year's forecasts take a strategic look into the key clusters and factors that will impact global security and stability.

1. Geopolitical
2. Geoeconomic
3. Societal
4. Environmental
5. Health
6. Technological
7. Psychological

*Kindly note that the numbered list was used with a sequence purpose and not as a ranking tool.

Geopolitical

Ukraine will continue to be the centre of attention for Europe, and remain the focal point for Moscow's existential battle with the West. China has been closely watching the West's response to the Ukraine war, factoring in valuable information into Beijing's strategic calculus regarding Taiwan. Instead of a full-on assault on mainland Taiwan, Beijing is likely to intensify provocations around disputed islands in the South China Sea and around Japan. In the Middle East, the JCPOA (or "Iran Nuclear Deal") is dead, but the government will continue to deal with a rising protest movement that may inspire another uprising for democracy and civil rights in the region, such as the Arab Spring movement that started in Tunisia in 2010. As food and energy costs rise and shortages deepen, coupled with reverses in democratic gains, the MENA, Sub-Saharan and Latin America regions will be vulnerable to anti-government convulsions.

The geopolitical landscape is constantly evolving, and at times abruptly and swiftly, creating risk trends that can be difficult to identify and monitor as well as impact the range of opportunities that risk professionals and businesses face. Shifts in geopolitics can arise from a change in governments, terrorism, war, pandemic, or natural disaster, and these have tangible impacts on investments, operations, and staff well-being. In our hyper-connected business world, businesses will need to understand their geopolitical risk exposure as part of their enterprise risk management processes to reduce uncertainties and to navigate through potentially challenging environments. Thus, it is important for risk management professionals, up-and-down the management chain, to map potential risks to tangible outcomes.

What should you consider for your organisation?

Factoring Geopolitical Risks

Organisations factoring in geopolitical risks into the ERM framework should focus in the following:

- **Decentralised decision-making:** Establish redundancies and resilience by divesting authority to regional offices. This will allow avoidance of delays for risk decisions that require an appreciation of the nuances of the local environment.
- **Assets in unstable environments:** Operating in volatile markets presents a higher degree of exposure to risk events, including war, terrorism, populist unrest and natural disasters, among others.
- **Employee and supply-chain mobility:** Natural disasters, pandemics and conflict can trigger abrupt shifts in government policies and protocols. Ensure contingency plans are dynamic and fit-for-purpose, factoring in scenarios for best practice planning.
- **Information and cyber security:** There are now stronger linkages between events taking place in the geopolitical and cyber space. Stay ahead of the developments in both with proactive monitoring of threat intelligence events.

Geoeconomic

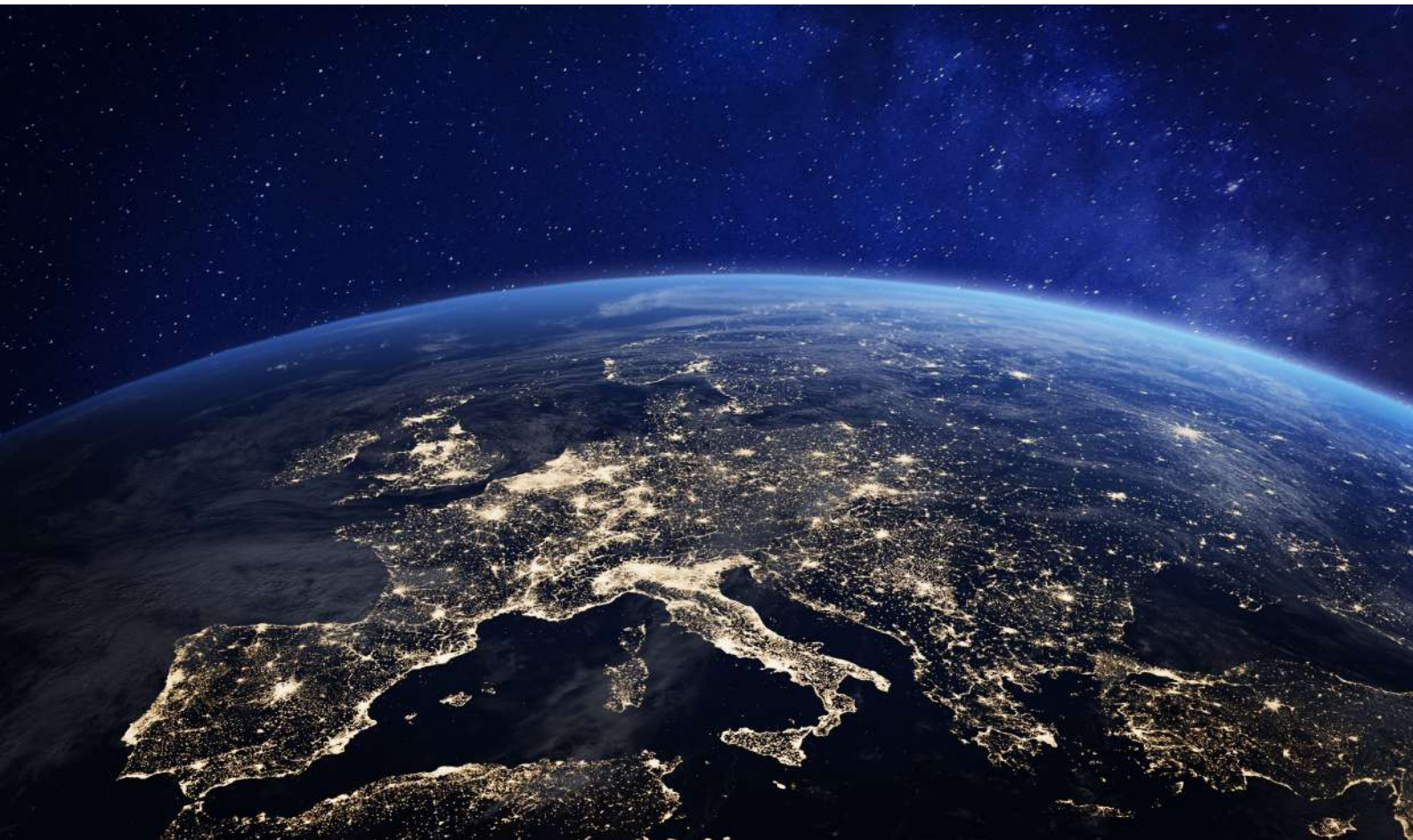
Global economies are set to face significant challenges from increasing inflationary pressures linked to the pandemic and Russia's war in Ukraine, and the subsequent weaponisation of trade. Sanctions and anti-competitive regulations have become the normative responses to geopolitical competition. A third of countries are expected to see their economies contract. Global debt is set to rise, likely exceeding the USD 303 trillion record set in 2021, and dragging more than 50 of the poorest states deeper into risk of bankruptcy. In Latin America, public discontent with governments will remain relatively as economic growth is expected drop to around 1.7%, according to the IMF. This means that governments will unlikely implement any economic measures that will incur disapproval from the citizenry, particularly in states with elections such as Argentina and Paraguay.

Negative economic environments and trends can have profound disruptive risks, potentially leading to long-term irreversible and varying damages. For firms, deteriorating economic conditions at the state-level can impact finances and operations, and the severity will be determined by the level of risk preparedness. At the macro-level, the COVID-19 pandemic and Ukraine war stressed the global supply chain, introducing severe shocks and heightening economic uncertainties. Even businesses that have been financially sound and competitive have been forced to take corrective actions to reduce the severity of any negative impacts.

What should you consider for your organisation?

Factoring Geoeconomic Risks

- **Enterprise Risk Management:** Because geoeconomic risks are transnational, firms need to have a global outlook and factor in international developments as part of an integrated enterprise risk management approach.
- **Tailored Intelligence:** Monitoring early warning indicators, such as foreign sanctions lists, import/export bans, outward/inward investment bans, anti-competitive legislation and decrees, market regulations, bureaucratic red-tape as well as state and non-state activities including industrial espionage and intellectual property theft. Economic indicators to monitor are debt/GDP ratios, inflation and interest rates, unemployment, and labour costs, among others.



Societal

Climate and pandemic related events, compounded by the geopolitical rivalries and antagonisms, will add more pressure on societies struggling economically. The continual undermining of economic livelihoods, rising poverty and worsening wealth inequality will raise the risk of political and societal violence, especially in states with weak institutional resilience and predatory political actors. Somalia, Ethiopia, Democratic Republic of Congo, South Sudan, Afghanistan, Yemen, and Haiti, among other will see further slide of social and political instability. There will also be pivotal elections in India, Pakistan, Bangladesh, Thailand, Cambodia and Myanmar.

Understanding the pulse of the local environment can be achieved through effective intelligence planning involving relevant stakeholders. Organisations with a better outlook on the societal factors will benefit from their efforts to anticipate, adapt and set the onsets for a faster approach on business opportunities.

What should you consider for your organisation?

Factoring Societal Risks

- **New Market Entry:** Prior to entering a new market, organisations should consider undertaking an assessment of the local environment to identify and priorities threats and risks from political, economic, legal, reputational, competitive, environmental and societal perspectives.
- **Corporate Social Responsibility (CSR):** An organisation's operations will have an impact on the local community and society. A CSR programme should link the objectives of the organisation with that of the expectations of local communities and stakeholders with an overall objective of reducing risks and raising opportunities.

Environment

Increasing global greenhouse gas emissions will make 2023 warmer than 2022. Global temperatures are forecast to reach at least on average 1.2C higher than pre-industrial (1850-1900) levels for the 10th consecutive year. This will impact agricultural production, supply chains and pricing, particularly in less resilient economies. 2023 will also be a transition year as La Niña phenomena in the tropical Pacific Ocean region will gradually give way to the warmer El Niño in the second half of the year. El Niño is expected to add more stress on the agricultural sector in parts of North America, SE Asia, and Sub-Saharan Africa.

Climate change poses multi-layered and varying risks to businesses, requiring firms to adopt more proactive, dynamic and holistic approaches to mitigating strategies.

What should you consider for your organisation?

Factoring Environmental Risks

There are some principles that companies should consider when developing these strategies, including but not limited to:

- Carry out broad-spectrum assessments, factoring in operations, products and services, to identify risks and opportunities.
- Create and implement thresholds for anticipated change and impact for those strategies.
- Have a flexible and innovative approach that allows for change in response to external pressures or sudden, unforeseen disruptions.
- Scenario plan to evaluate multiple strategic plans.
- Internal marketing to raise awareness on climate change strategies, policies and plans to get stakeholder buy in.

Health

The world is better prepared for COVID, and the pandemic is likely to recede further into 2023 barring the emergence of a more virulent strain. China is in the beginning phases of experiencing a surge in Omicron cases as Beijing eased restrictions in response to widespread anti-lockdown unrest. Around 60% of its population (or around 800 million people) are likely to get infected during the first quarter of 2023. Undoubtedly there will be spillover into other states, and those states with gaps in testing and low vaccination rates will provide optimal conditions for the emergence of variants. Climate change-related animal encounters will also likely see the emergence of new viruses, including pathogens that can jump species, and potentially impact animal and human welfare, particularly in Africa and Southeast Asia.

The pandemic presented multiple challenges to the staff of organisations, as it upended the operating model for businesses and forced them to make difficult decisions. While organisations have known that they have a duty of care to ensure the physical safety and mental well-being of their staff, the pandemic has illustrated how critical it is to fulfill their respective obligations.

What should you consider for your organisation?

Factoring Health Risks

To get ahead of a development before it becomes an incident, risk managers can consider the following:

- **Predictive analytics:** Use tools that help analyse health and mobility-related risk intelligence data to help enable and improve risk management and decision support.
- **Scenario planning:** Scenarios and related exercises help risk managers work through potential worst-case events, with learning outcomes allowing organisations to address vulnerabilities.
- **Monitoring:** Health, Safety, Security and Environment teams should monitor indicators and warnings that allows managers to executive decisions effectively and efficiently.
- **Crisis Management and Communications:** Ensure that crisis management and communication plans involve relevant stakeholders across the organisation and are reviewed periodically to ensure effectiveness. Have a plan that is clear, succinct and adaptable.

Technological

Cyber threat actors, both state and non-state sponsored, will continue to evolve tactics, posing higher levels of risks to governments, businesses and society. Ransomware will remain the number 1 risk. For businesses that have adopted hybrid or remote work structures, their workforce will be more vulnerable to business email compromise attacks. As more organisations utilise cloud networks, there will be a natural evolution to targeting these environments. Misinformation and disinformation campaigns will continue to have its disruptive effects on society, politics and businesses, forcing governments to impose tighter regulatory measures on social media companies.

Cyber security should be a shared responsibility across the enterprise, particularly given the shift towards remote and hybrid work models that have pushed organisations to scale up digitisation of business processes. Policies, plans and processes can take many shapes, depending on an organisations requirements and resources.

What should you consider for your organisation?

Factoring Technological Risks

Here are some recommendations to consider:

- **Third-Party Vendors:** Thorough vetting and auditing of third-party is a must to mitigate risks associated with intellectual property, personnel and customer data, as well as financial information.
- **Cyber Threat Intelligence:** Proactive identification and monitoring of emerging threats, or new regulations, will help organisations prepare for a cyber event.
- **Testing:** Periodic stress or vulnerability testing of an organisation's digital infrastructure will identify the level of preparedness for any adverse events. Weaknesses can be addressed, and new policies and processes can be development and conveyed to staff.
- **Security Awareness and Training:** The continual evolution of the cyber threat landscape, including the emergence of new attack trends, requires organisations to prepare staff with the equipment, software and training to mitigate those threats. Initial training during the onboarding process should also be followed up with periodic awareness training to ensure best practices are followed.

Psychological

COVID-19 created an environment of uncertainty and triggered seismic shifts in the way organisations conduct their activities. Organisations were also forced to focus greater attention on the mental well-being of their workforce. While there was cautious optimism that the fog of the pandemic would lift, the onset of the Ukraine war and its ramifications on global economies added multiple layers of stress on businesses and societies.

A study run by the American Psychological Association (APA) in February 2022 underlined that the top sources of stress among the population had been the rise in prices (87%), followed by supply chain issues (88%) and global uncertainty (81%). A subsequent APA study in March 2022 had ranked the global uncertainty (81%), the Russian invasion of Ukraine (80%) and the potential retaliation from Russia via cyber or nuclear (80%), as the most troubling stresses for American society. Indicators and warnings heading into 2023, strongly suggest more turbulence caused by global health, climate, geopolitical and geoeconomic events that will likely mean that anxiety levels among societies will remain comparatively high. And this will have implications on local stability and security dynamics.

What should you consider for your organisation?

Factoring Psychological Risks

Organisation looking to ensure positive mental well-being and stability of their workforce, could consider the following:

- **Organisational Culture:** Ensure good transparency when communicating the organisation's visions, objectives, strategies and plans to reduce the level of uncertainty and anxiety of personnel.
- **Supportive Sessions:** An organisation's number one asset is its people. Promote a positive risk culture and encourage stakeholder engagement and ownership of decision-making processes up-and-down the organisation. Prepare your staff for crisis through training, including sessions about post-crisis mental well-being. Provide them with access to mental health specialists and the opportunity to engage with these specialists in a safe and secure manner.

Conclusions

The key question that businesses should be asking is whether they are prepared to navigate through another year of turbulence and challenging risk environments in 2023.

Political, geopolitical and geoeconomic shocks will continue to define the risk landscape but in less uniform ways as certain countries become more resilient in their responses while others will still struggle to catch up. The Ukraine conflict and its side effects will drag on in 2023 with little substantive indicators for settling the conflict. Instability in the Middle East, Latin America and Sub-Saharan Africa also has the potential to disrupt markets. China-US relations will shape stability beyond the Asia Pacific as the former looks to rebound from the pandemic. Thematically, the cyber domain will become increasingly perilous for governments, businesses and societies, with a rising number of threat actors seeking financial and political concessions.

There is room for cautious optimism, particularly among states and organisations that have applied lessons learned; however, this optimism should not segue into complacency.

If you are interested in monitoring risks affecting your organisation, reach us at support@nssg.global