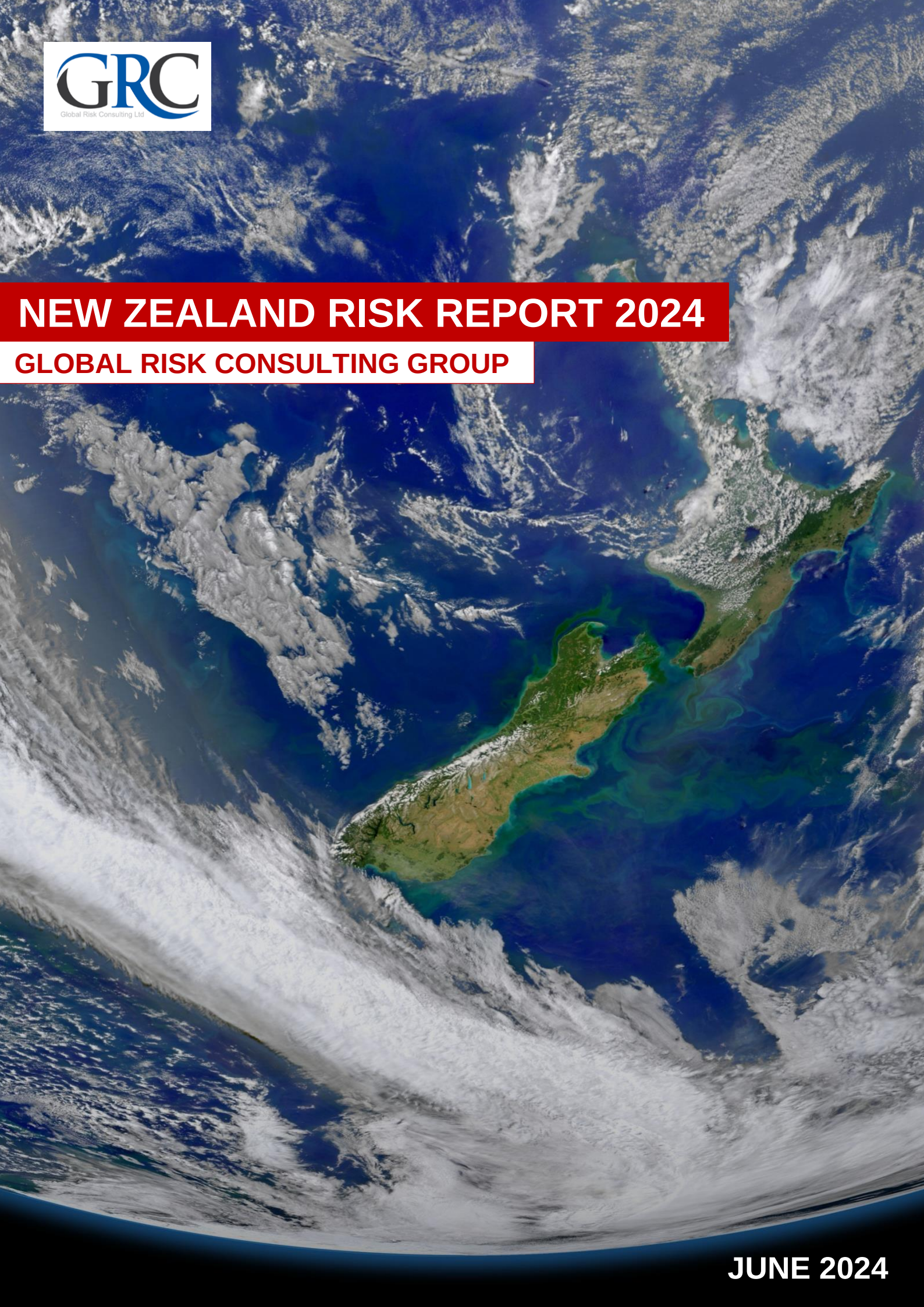


NEW ZEALAND RISK REPORT 2024

GLOBAL RISK CONSULTING GROUP

JUNE 2024

[DISCLAIMER]

This report is general in its application and some analysis may be subjective. While every effort has been made to ensure the accuracy of the report, no liability whatsoever can be accepted for any error. The findings in this report do not necessarily reflect official policy or position of GRC Group. Examples presented within this report are for the purpose of demonstration.

It is recommended that users carefully evaluate the accuracy, currency, completeness and relevance of the material for their purposes. This information is not a substitute for independent professional advice and users should obtain any appropriate professional advice relevant to their circumstances.

Publication Details

Version	Date	Status
1.0	23/05/2024	Initial release
2.0	1/06/2024	Full release

Released June 2024

CONTENTS

1. PREFACE

As we emerge into the 'post-COVID' world we find uncertainty and 'wicked problems' are abounding, and there is a greater need than ever to navigate interconnected risks intelligently, inclusively, and sustainably. It is crucial to understand that the challenges we encounter do not exist in isolation but are part of a larger, intertwined risk landscape that extends off our shores. The 2024 New Zealand Security Risk Report builds on the foundations of its predecessor to offer a far more comprehensive, holistic view of security risks and hazards, what's driving them, how likely they are, and what the nature and magnitude of consequences may be to different 'layers' of society.

The ISO:31000 remains central to our risk management approach, and is enhanced in 2024 by the IEC:31010 (risk assessment techniques) and the HB 167 (security risk management). These standards, combined with horizon scanning, the *Impact-Uncertainty Matrix*, and the GRC *Hazard Layer Model*, offer a robust analytical process that gleans deep insights about how our whanau (families), tangata (people), businesses, wider communities, and natural environments experience insecurity.

Our report is structured in such a way that each chapter provides context for the next, beginning with the expansive overarching risk profiles of Global Strategic Competition and Climate Change and Natural Disasters, narrowing the scope into the more technical disciplines of Emerging and Sensitive Technology, Foreign Interference, and Critical Infrastructure Vulnerability, then dialling-in to specific risks surrounding Terrorism and Violent Extremism, Cyber and Digital Threats, and Transnational Organised Crime. Each chapter identifies, analyses, and evaluates six critical sub-risks, offering our readers a nuanced understanding of how these hazards can affect different aspects of life in New Zealand.

Our objective is to present an authoritative analysis that is guided by international thinking, inspired by our team's experience, informed by global best practice, achieves a fine balance of internal and external threats, and offers a unique and informed New Zealand perspective on some of the major security risks facing not only our nation, but the global community.

Chris Kumeroa
Managing Director
Global Risk Consulting Group
chris.kumeroa@globalrisk.co.nz

secintel Manaaki CMS GRC Group Systems safehome

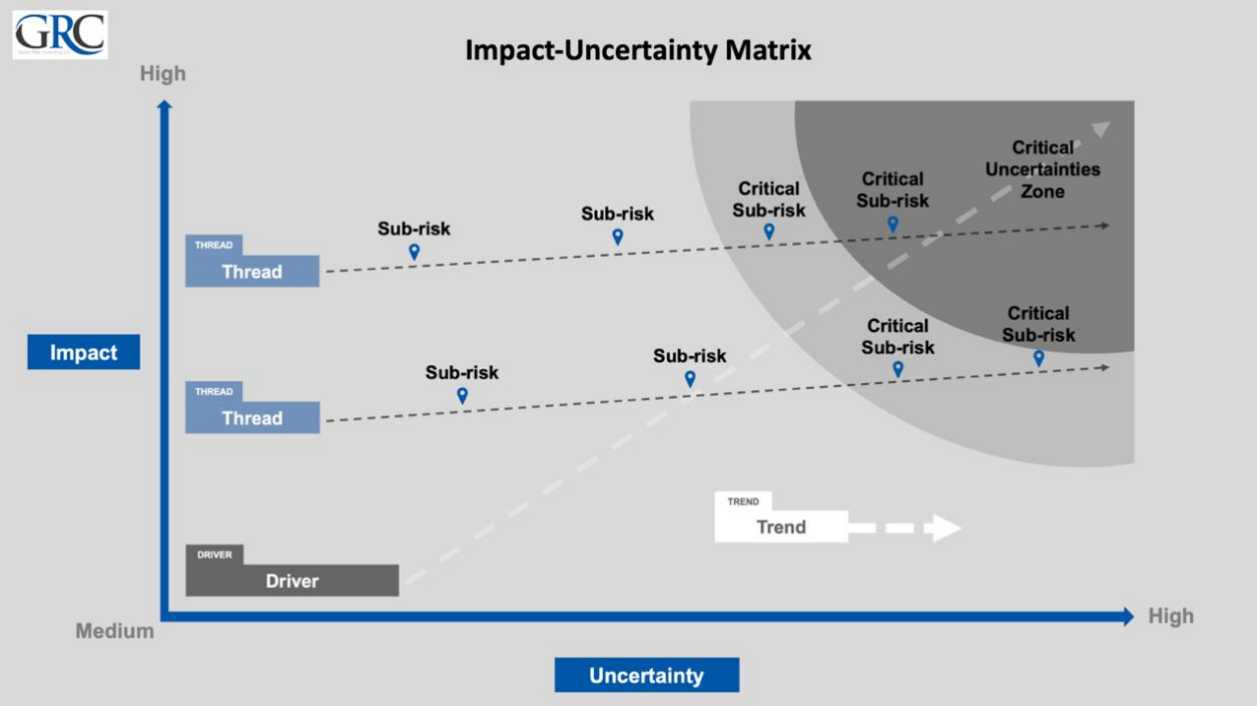
2. METHODOLOGY

The 2024 Risk Report identifies security risks to New Zealand and the potential consequences to the nation's people, economy, national security, environment, and reputation. The report pulls from academic journals, government reports, policy documents, NGO resources, news sites, and open-source intelligence sources. This year we developed and refined our methodology to follow a comprehensive three-step process: Horizon Scanning to develop an Impact-Uncertainty Matrix, pushing the Critical Uncertainties through a Risk Management process, then applying the Hazard Layer Model to discover consequences to different, but connected, layers of society. Through this we hope to achieve a detailed, nuanced, security-focussed qualitative analysis that stimulates discussions and opens up avenues of exploration.

2.1. The Impact-Uncertainty Matrix:

After scanning the horizon and identifying multiple sub-risks within the overarching risk profile we plot them on the Matrix. The Y axis measures the potential impact of a sub-risk and the X axis measures the uncertainty you have about how this sub-risk may develop in the future. The dark grey area in the top right-hand corner of the model is the **Critical Uncertainties Zone**, representing the sub-risks that may have the highest impact on New Zealand and the most uncertainty about how and when this may happen.

Based on horizon scanning and analysis we identify three **Threads** which can be interpreted as categories or avenues through which the overarching risk profile manifests in different ways. This methodology allows us to 'pull threads' within a larger risk profile to unpack complexities, discover interconnected sub-risks, and find blind spots. A **Driver** is added to the model for a better visualisation of what is pushing risks forward, and a **Trend** may be added to represent other background forces or impacts. A finished matrix is a good representation of the strategic environment surrounding a risk profile and provides opportunities for further assessment and design of controls for specific problems.



2.2. Risk Management Process:

The 2024 Risk Report more closely follows the international standards of ISO:31000 Risk Management Process, IEC:31010 Risk Assessment Techniques, and HB 167 Security Risk Management. Our methodology takes the top six sub-risks inside the Critical Uncertainties Zone and applies a streamlined four-step risk assessment based on the ISO:31000:

1. **Context and Scope:** Introduces the overarching risk profile and sub-risks, establishes the context of the analysis, discusses the Macro Risk Drivers influencing it, and sets the scope of the assessment.
2. **Risk Identification:** How we describe the sub-risks and how we have identified them as risks.
3. **Risk Analysis:** Based on the nature and level of risk we apply likelihood ratings, guided by the NZSIS probabilistic language scale, and analyse current and potential impacts.
4. **Risk Evaluation:** Based on the above analysis we discuss what risks are acceptable, tolerable, or unacceptable and discuss why.
5. **Hazard Layer Model (HLM):** We then apply our findings to the HLM to see what Layers of society are impacted, and how.

Our Risk Analysis step employs an expanded version of the NZSIS probabilistic language scale which separates '*Possibly, Realistic Possibility 25-50%*' and '*Likely, Probably 55-70%*' into four categories in order to offer more nuance in our likelihood ratings:

- Highly unlikely 1-10%
- Unlikely 15-20%
- Possibly 25-35%
- Realistic possibility 40-50%
- Likely 55-60%
- Probably 65-70%
- Highly likely 75-85%
- Almost certain 90-99%.

Methodology notes:

Given the broad, qualitative, and open-ended nature of many of the overarching risk profiles and sub-risks within them, and this report being an external research and analysis resource intended to provide value for a large audience rather than a risk assessment conducted for a client internally, our methodology does not adhere to every step in the ISO:31000 or other standards. For example, it does not make distinctions between external and internal context or offer criteria for every risk during Risk Identification, it does not discuss Preventative, Detective, or Corrective Controls during Risk Analysis, it does not suggest decisions during Risk Evaluation, and does not complete a Risk Treatment step. Where appropriate throughout the report we utilise tools from the HB 167 Security Risk Management standard such as considering Root Causes, Dynamic Pressures, and Unsafe Conditions related to risks, Criticality Assessment and Vulnerability Analysis of critical infrastructure, or Threat Assessment of violent extremist groups.

It is also important to note that it is beyond the scope of this report to advise or make recommendations on foreign policy, defence policy, and economic policy. Instead, it presents the risks as they stand now and how they may look in several years, with a focus on using the Hazard Layer Model as an ordering framework for consequences to New Zealand. Thus, this is not a technical paper and does not seek to empirically prove or disprove the likelihood or impact of risks, nor does it offer a list of recommendations strategic decisions, policy actions or resource allocations.

2.3. Hazard Layer Model:

The HLM considers the hazard-scape in terms of seven interlinked hazard 'layers'. Although these layers bear some similarities with security and resilience categories found in the UN 'Human Security' model, the New Zealand Government 'all hazards' approach, and the NZ National Emergency Management Agency (NEMA) 'Model of a Resilient Nation', they are a unique *layering* (as opposed to a *categorisation*) of hazard spaces from the perspective of the individual.

As individuals, we inhabit multiple spaces, from our homes to our towns and workplaces, to the natural environment around us, and our individual experience of these spaces and the hazards we might be exposed to in these spaces is unique. For some, the home might be the space of greatest hazard exposure due to family harm or a lack of basic life necessities, while for others, the prevalence of retail crime in their community may present a disproportionate exposure.

The HLM can be considered *an ordering framework for consequences* and facilitates a local, data-driven understanding of the multi-layered individual implications of the big risks and threats.

The seven hazard layers of the HLM are:

1. Individual
In or of the person, including perceptions of insecurity, mental and physical health issues, issues of identity and belonging.

2. Residential
Within the home, including inadequate living conditions, deprivation, parental neglect, and family harm.

3. Accidental
Misadventure at work and at play, including transport, water safety, and workplace health and safety incidents.

4. Societal
Within the community, including antisocial behaviours, crime, cybercrime, bullying, and harassment.

5. Ideological
Within public discourse, including mis/dis-information, identity or ideologically motivated hate, political violence, terrorism, espionage and foreign interference.

6. Biological
Within our air or food chains, including epidemics, pandemics, and other public health incidents, contamination and biosecurity incidents.

7. Environmental
In the environment, including extreme climatic, hydrological, and geological events, and the effects of climate change.

2.4. Macro Risk Drivers (MRD)

The overarching risk profiles explored in this report, and many of their sub-risks, are often highly qualitative, open-ended, and of significant import to a wide array of actors, stakeholders, industries and timeframes. Inherently they are 'wicked problems' in which trying to understand or solve them typically produces more questions than answers. To navigate this our analysis identifies macro-level drivers that connect and amplify the risks and hazards we face. This enables us to apply a structure to complex and sometimes nebulous global trends, understanding how they are being pushed and in what direction, and dial down from broad to specific risk profiles where we can produce more pragmatic impact-level assessments. This also allows us to engage in strategic foresight so that we may better understand how emerging risks may influence the strategic environment and what their consequences could be over a longer time horizon. This is not a strict analytical model, instead it serves to establish guiderails and acts as an indicator of the direction and intensity of the larger forces driving risk.

2.4.1. Geopolitical Instability

Competition between states economically, politically, technologically, and socially is a normal function of the international rules-based system and can be mutually beneficial, and even encouraged to deepen ties such as international sport and technological innovation. However, the emerging multipolar power structure, undermining of democratic processes, degradation of international institutions, expansion of foreign interference operations, the emerging cyber and information battlegrounds, natural resource deficits, and proliferating inter-state conflicts herald an era of unstable, strategic, and zero-sum competition. EY reports that 'mentions of geopolitics and political risk in companies' public documents skyrocketed 600% in 2022' and remained elevated in 2023.[1] In 2024 we are seeing a 'global elections supercycle' in which 54% of the world's population, representing 60% of global GDP, will go to the polls, raising the risks of polarisation, social unrest, and regulatory and policy uncertainty.[2] Revisionism, economic protectionism and authoritarianism are on the rise as China, Russia, Iran, North Korea and their allies deepen their ties, consolidate resources, and align foreign policy and defence objectives to shape the international order to suit their interests. Political instability in parts of Eastern Europe, South America, the Middle East, and Africa open opportunities for revisionist powers to pull weaker, unstable states further away from the US-led rules-based international system and into the emerging Non-Western Axis which promises more favourable economic and political paradigms. Geopolitical Instability is a driver of Global Strategic Competition, Foreign Interference, Cyber Threats and some Emerging and Sensitive Technology.

2.4.2. Post-COVID Social Unrest

The COVID-19 pandemic triggered a sharp rise in social unrest and incivility around the world. The Global Peace Index reported that there were 14,871 violent demonstrations, protests and riots recorded globally in 2020, and over 60% of people around the world report being worried about sustaining harm from crime and unrest.[3] In New Zealand there has been a considerable increase in violent and dehumanising rhetoric towards politicians, media personalities, ethnic minorities, gender minorities, women, migrants and other groups. Disinformation, conspiracy theories, anti-authority sentiment and international tensions are compounding with cost of living and housing crises and high unemployment, leading to a regular social and political flashpoints where large groups voice their dissatisfaction through petitions, protests, counter-protests, rallies, activism, threats, harassment, intimidation, vandalism, crime and in some cases violence. Post-COVID Social Unrest is a driver of Terrorism and Violent Extremism, Digital Threats, and Transnational Organised Crime.

2.4.3. Rapid Technological Change

The rapid advancement of technology presents major opportunities and risks that permeate every all aspects of society. At the front of the public consciousness is Artificial Intelligence (AI), which has

proliferated at an unprecedented pace since 2022 and is already utilised in every major industry. Developing in the background, however, and often overshadowed by AI, are major maturations in semiconductor production, robotics, nanotechnology, directed energy beams, space and counterspace technology, quantum computing, biotechnology, and more. In several critical areas these technologies are advancing faster than policies designed to regulate them, and concerns about dual-use dilemmas, ethics and governance will be a key socio-political and economic issue over the next decade. Rapid Technological Change is a driver of Emerging and Sensitive Technology and Cyber and Digital Threats.

2.4.4. Climate Change

Climate change, particularly warming, is having an amplifying effect on a range of other risk profiles. As natural environments undergo degradation they become more vulnerable to climate change-related impacts such as sea-level rise or cessation of ecosystem services, and are less resilient to natural disasters. This is making fluctuations in temperature and related natural disasters like storms, floods and droughts more extreme, increasing pressures on the natural systems we rely upon for economic stability. The varying degrees of exposure to natural hazards across New Zealand's regions, cities, sectors and communities alongside complex and often unforeseeable consequences makes risk assessment and crisis response planning difficult. Direct impacts ranging from property damage to permanent ecosystem change extrapolate over time and combine with other climate stressors to create migration pressures, economic instability, compounding health crises, and more. While Climate Change is a MRD in and of itself, it is also pragmatic to assess it as a risk profile focused primarily on environmental degradation and natural disasters. Therefore, Climate Change is a driver of Climate Change and Natural Disasters, Critical Infrastructure Vulnerability, and to an extent Global Strategic Competition.

3. RISK EVALUATION SUMMARY

ACCEPTABLE	TOLERABLE	UNACCEPTABLE
Global Strategic Competition: - Sovereign Digital Spheres Climate Change & Natural Disasters: - Permafrost Thaw Emerging & Sensitive Technology: - AI Ethics & Governance - Quantum Information Science	Global Strategic Competition: - Logistics Vulnerability - Resource Scarcity - Artificial Intelligence - Space & Counterspace Climate Change & Natural Disasters: - Ecosystem Change - Negative Health Outcomes - Compounding Health Crises - Political Instability Emerging & Sensitive Technology: - Dual-Use Dilemmas - Orbital Dominance Race - Biomedical Technology - AGI Foreign Interference: - Critical Industry Leverage Critical Infrastructure Vulnerability: - Regulatory Resilience Gap - Espionage & Sabotage Terrorism & Violent Extremism: - Identity MVE - M.U.U. - Foreign Support Networks Cyber & Digital Threats: - Synthetic Media Epidemic - Oppressive Algorithms - Cyber-Physical Attack - Data Centre Security Transnational Organised Crime: - Justice System Strain - Local Economic Pressures - Intergenerational Cycle	Global Strategic Competition: - Malign Influence Operations Climate Change & Natural Disasters: - Extreme Weather Patterns Foreign Interference: - Eroding Public Trust - Exploiting Sensitive Research - Industrial Espionage - Engineering Social Sentiment - Disinformation Campaigns Critical Infrastructure Vulnerability: - Crisis Response Lag - Cascading Failures - Earthquake - Compound Disaster Terrorism & Violent Extremism: - Disinformation - Complex Attack - CBRN Attack Cyber & Digital Threats: - Hackers For Hire - Vendor Data Exposure Transnational Organised Crime: - Cross-Border Collaboration - Evolving Tactics - 501s Amplifying Capability
Total: 4	**Total: 25**	**Total: 19**

[1] EY. Courtney Rickert McCaffrey, Oliver Jones, Famke Krumbmüller. 'Top 10 Geopolitical Risks for 2024'. 12 December 2023. https://www.ey.com/en_gl/insights/geostrategy/2024-geostrategic-outlook.

[2] Ibid.

[3] 'Civil Unrest and Political Instability Increases Due to COVID-19'. Vision of Humanity, 17 June 2021. https://www.visionofhumanity.org/world-less-peaceful-as-civil-unrest-and-political-instability-increases-due-to-covid-19-pandemic/.