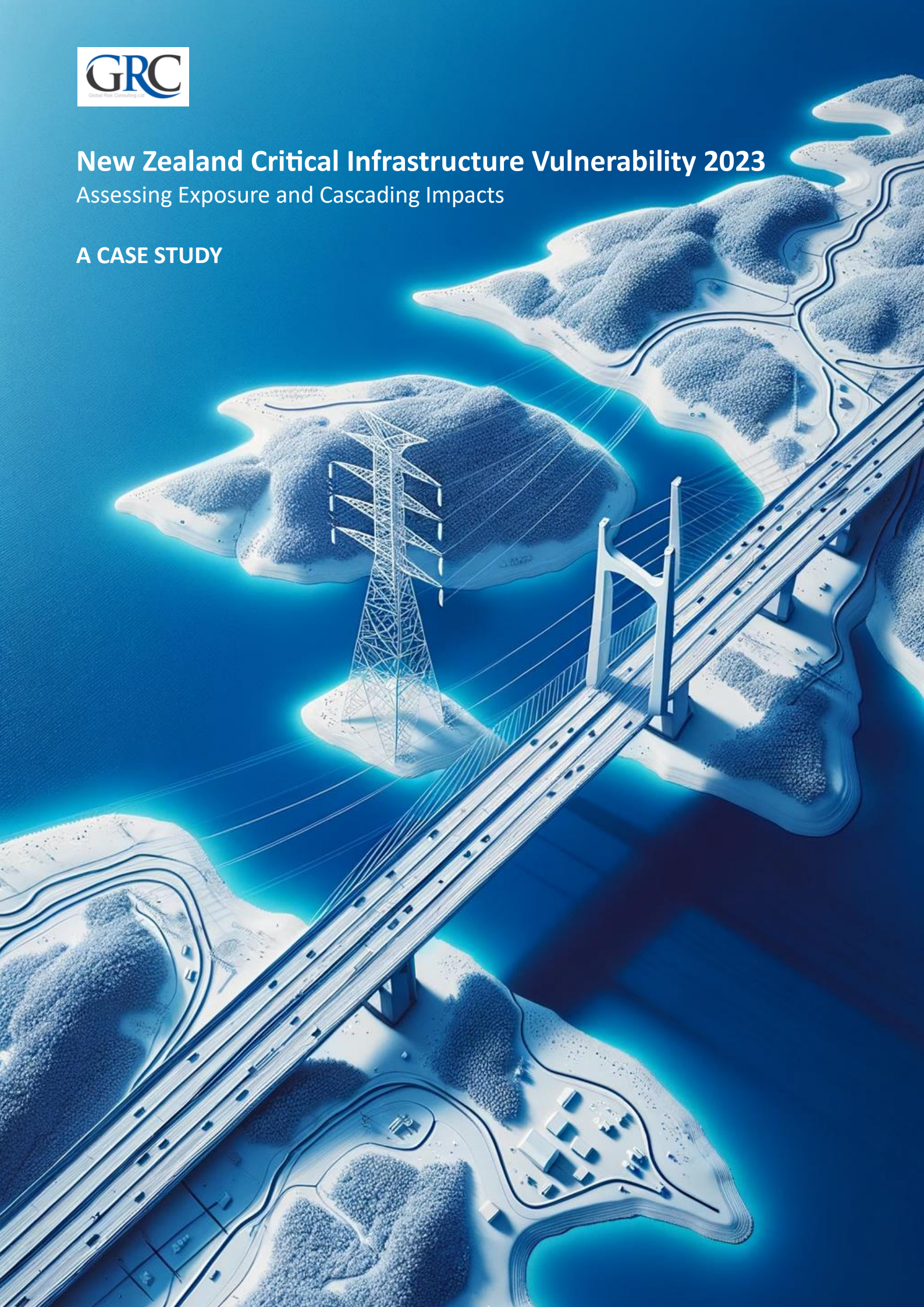
New Zealand Critical Infrastructure Vulnerability 2023

Assessing Exposure and Cascading Impacts

A CASE STUDY



A major risk to the safety and security of New Zealand is disruption to critical lifelines infrastructure. In the context of risks and hazards, 'Nationally Significant' infrastructure assets are 'often where there are single-site 'pinchpoints' in the supply chain which, if they failed catastrophically, would cause a significant loss of service'. Understanding how different hazards could affect nationally significant critical infrastructure is a challenge in and of itself. Focus typically falls on immediate, direct impacts but the Lifelines Council emphasise the need for deeper analysis of the 'composite, cascading, and cumulative nature of hazards'. This is not only true for the damage and the cascading, cross-sector impacts through critical lifelines themselves, but also for the flow-on impacts on functioning of government and business, critical supply chains, civil defence, and social cohesion.

Critical lifelines infrastructure refers to Electricity Generation, storage, and distribution (hydro, power stations, power pylons, wind turbines, coal), Fuel and Gas (plants, tank farms, pipelines, ports for fuel import), Roads, Air Transport, Rail Transport, Sea Transport, Telecommunications, and Water. Many of these such as pipelines, roads, bridges, and railways are 'long, linear assets spanning variable terrain, often in remote locations' and are particularly vulnerable to seismic movements, slips, landslides, coastal inundation, and erosion.

Complex interdependencies between these systems amplify the consequences of natural disasters by triggering 'cascading' impacts throughout various infrastructure networks and sectors. In 2011 a landslide at the Pukearuhe site in Taranaki caused the Maui gas pipeline to rupture, with MBIE later estimating that this disruption cost the region, and wider North Island, over $200 million. Without gas, farmers in the region were unable to process milk and some reportedly dumped their supply into nearby waterways, leading to localised environmental impacts. The Counties Manukau District Health Board's SuperClinic also had to cancel several surgeries, leading to an investigation on how gas companies can better communicate information to critical health services during an emergency.

The scale of the cascading impacts from disruption to lifelines varies greatly by region and is difficult to quantify. For example, a large earthquake in Wellington could severely damage the mains transporting water from critical aquifers into the city proper and is estimated to take months to repair. Christchurch's water supply, however, is more resilient due to its more numerous and distributed aquifers in the surrounding areas. Auckland Airport is threatened by flooding, sea level rise, and coastal erosion, whereas Queenstown Airport is threatened by the Alpine Fault line and limited on-site fuel reserves in an emergency.

Repairs to the Maui pipeline in Taranaki, 2011 – Cameron Burnell/Stuff

… pipelines, roads, bridges, and railways are long, linear assets spanning variable terrain, often in remote locations…

New Zealand is one of the most disaster-prone countries in the world, and our high levels of exposure to natural hazards tend to dominate discussions around critical infrastructure vulnerability and how to regulate and build for resilience. This de-prioritises analysis of another critical threat profile: Sabotage and Espionage. In November 2022 Graham Philip became the first person in New Zealand history to be charged with sabotage after he intentionally damaged Transpower infrastructure in late 2021, reportedly causing over $1.2 million in damage while attempting to cut power to the entire North Island. Philip was fervently against vaccine mandates, “a matter that concerned him greatly”, and in the words of his lawyer believed that “the view of those who oppose government actions weren’t being heard… something needed to be done.” He pleaded guilty to seven charges of sabotage, one charge of entering agricultural land with intent to commit an imprisonable offence, and on December 1st he was sentenced to three years and one month’s imprisonment.

This case exemplified how ideologically-driven sabotage is an emerging threat to our critical infrastructure. This raises questions about not only assessing how critical infrastructure fits into the violent extremism motivation picture, but also how design, architecture, and physical accessibility needs to be re-assessed through a security lens. Easy access to an asset is essential for regular checks, maintenance, and repairs during an emergency, but this becomes a double-edged sword when considering how malicious actors may carry out target selection and weak-spot assessments. Furthermore, the threat of eco-terrorism (violent acts motivated by environmentalist beliefs) against fossil fuel infrastructure and other perceived polluters is increasing as environmental degradation continues globally.

New Zealand’s critical infrastructure may also be a target of espionage or sabotage by foreign states, strategic competitors, or state-sponsored actors. These groups may seek to monitor, disrupt, damage, or hack certain systems to gather intelligence, gain economic advantage, gain political leverage, or conduct counter-intelligence to protect themselves. A key concern here is cyber-physical attacks in which an actor infiltrates the technological back-end that monitors and regulates an infrastructure asset (cyber-attack) and gains control of physical systems. The most famous example of this was Stuxnet, a computer worm virus that accessed the IT system of an Iranian nuclear facility in 2007 which shut down physical cooling systems, causing enormous damage to the facility and Iran’s wider nuclear program. In New Zealand’s context, such an attack could target water treatment plants, raisable bridges, or traffic management systems.

Hypothetic scenario/AI image: A hydro-electric power station in Southland hit by saboteurs

… this becomes a double-edged sword when considering how malicious actors may carry out target selection and weak-spot assessment…

Vulnerability and Security Considerations:

1. Widen use of geo-spatial data and deepen understanding of hazard-scape to model vulnerability. E.g., predicted flooding zones for sub-stations near waterways, or overlay geotechnical engineering assessments with seismic modelling to predict landslides onto roads and railways.

2. Comprehensive interdependence and redundancy assessments of critical systems to determine what the cascading impacts of a natural disaster or other threat may be. Combine this with forecasting/futures modelling for blind-spot analysis of second, third, and fourth-order environmental and social consequences.

3. Review regulatory approach to optimise for resilience: we need clear lines of communication and accountability between infrastructure owners/operators, government agencies, district and regional councils, Iwi, the public, and other stakeholders. Additionally, work to address systems hindered by historic underinvestment.

4. Robust and self-reinforcing security systems and protocols to deter emerging threats. Increased surveillance of critical assets and sites such as CCTV, human presence, and drone perimeter patrols; improved architectural and mechanical integrity; develop and regularly drill emergency response plans.

5. Enhanced intelligence cooperation between government agencies, emergency services, law enforcement, the private sector, and the public. Develop a Common Operating Picture (COP) and shared understanding of the natural hazard and emerging threat environment.

6. Build a comprehensive understanding of the foreign interference and espionage threat picture. Analyse case studies of cyber-physical attacks and intelligence gathering against critical infrastructure systems overseas, and leverage Five Eyes partnerships for preparedness and mitigation.

Widen use of geo-spatial data and deepen understanding of the hazard-scape to model vulnerability…

Contact: Chris Kumeroa, Managing Director | GRC Group | chris.kumeroa@globalrisk.co.nz