MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HIKINA WHAKATUTUKI

Telecommunications Resilience Review

NZ National Lifelines Forum – Auckland

Charles Jarvie, MBIE

Context - NZ's telecommunications infrastructure and services

- Challenges associated with building fibre optic links in rugged, narrow and sparsely populated geography
- New Zealanders well-served in terms of coverage and quality of service
- Small market dictates sharing of high cost infrastructure rather than duplication
- High level of responsiveness by operators - when interruptions to services do happen they tend to be localised and short in duration

Background – and what initiated the review

- Kaikoura earthquake:
  - Despite the extreme magnitude of the event, telecommunication services disruption was mostly confined to a lightly populated area of NZ
    - notable exception - 111 services disrupted for ~40 minutes
  - Industry players cooperated to restore local services, rearrange networks, coordinate logistics and repair damaged infrastructure
  - Generally staff resources were available but their deployment was made difficult by travel constraints – physical and procedural
  - Uncovered a network vulnerability that elevated the risk of losing South Island services south of Nelson and Blenheim
- Highlighted the need to better understand the sector's shared or common risks and how those risks might impact services to New Zealanders if they crystallised

Purpose and Method

"Assess the resilience of New Zealand's national telecommunications services to natural disaster events"

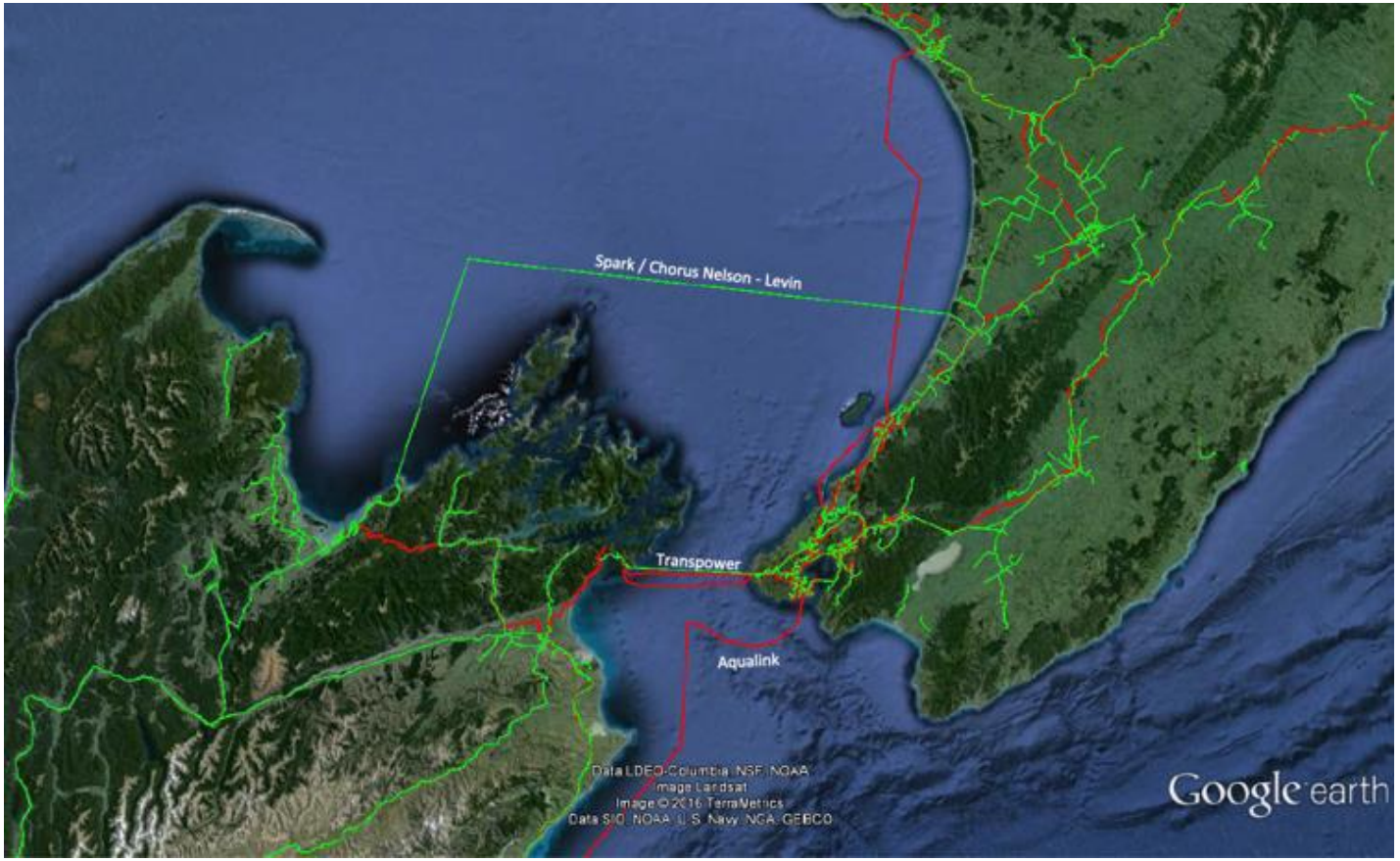
- Identify key nodes and links shared by operators
- Identify any coincidence with known natural hazard locations and understand the estimated return period(s) of the risk(s)
  - Seismic
  - Flooding
  - Landslip
  - Tsunami/inundation
  - Volcanic
  - Fire
  - Severe weather
- Share with contributing operators

What is out of scope?

- The review is not an audit of individual operators' network infrastructure and architectures
  - Operators' have multiple service platforms with complex interactions
  - Service architectures are continually changing
  - Accessing detailed commercially sensitive "traffic" information does not improve, and potential confounds, understanding of the basic underlying shared risks and their potential mitigations ("In general it is better to be approximately right rather than precisely wrong")
- Risks due to human factors, software and hardware failure, configuration errors, cyber security breaches and deliberate damage are excluded
  - These risks are generally uncorrelated between operators
  - These risks are best managed by operators
- Broadcasting services are excluded

Diversity around a bottleneck risk

An example of route diversity and correlated risk exposure



Next Steps

- Complete the data gathering phase with operators
- Identify key (high shared failure impact) nodes and links
- Overlay with natural hazards data sets
- Document the identified coincident risks and their estimated return periods
- Seek views on likely restoration approaches and mitigation options that may be appropriate