Submission on Strengthening the resilience of Aotearoa New Zealand's critical infrastructure system

Introduction and qualifications

- My name is Lindsay J Robertson. This submission is made on my own behalf, as a private individual.
- I am a New Zealand citizen, resident in New Zealand.
- I hold a PhD from University of Wollongong's Faculty of Engineering and Information Sciences. My thesis was titled "Identifying and reducing technological contributions to end-user vulnerability". I hold MTech (computing tech), and BE(Mech). I hold Fellow grade within IPENZ (Engineering NZ) and also within IMechE (UK). I am a chartered engineer (CEng UK) and IntPE.
- My publications on themes relevant to this submission, may be found in my ORCID record <https://orcid.org/0000-0001-9479-5251>. I would particularly note that I am first author of the IAIA best practice guide on resilience assessment <https://www.iaia.org/uploads/pdf/SP11%20Resilience.pdf>
- I would be willing to correspond to clarify any details, and I'd be willing to assist further if appropriate.

SUBMISSION

Abstract.

This submission:

- Recognises the breadth of concepts called "resilience" and notes the necessity to clarify the outcomes that are actually sought.
- Proposes that it is possible to define "critical infrastructure" whether this is provided by public or private sector.
- Notes the need for well-defined standards of resilience, that are linked to specific concepts of resilience.
- Recognises that many essential infrastructural services are provided by the private sector, who have distinctly different drivers from pubic sector, and proposes that there is an urgent need for a clear and future-proof approach to imposing resilience standards and to funding these.
- Proposes that there is a need to avoid, at all costs, any loss of "fallback" infrastructural functionality, and that this avoidance can be a matter of public policy.

1. Agreement on 'Resilience'

I have no desire to argue terminology or semantics, but without clarity on the goal, much effort will be dissipated without any useful result. I illustrate this issue by reference to a lecture I attended some time ago. The lecture was titled "improving the resilience of the roading system": I could have expected to hear about standardising road-repair materials and equipment/techniques, and about arranging local stockpiles to allow a damaged road to more rapid "bounce back" from a failure, but instead I heard about the importance of having more than one route between "A" and "B". Both approaches need consideration, but the "design redundancy" approach is expensive and depends on an assumption that one optional route is immune from the hazards that affect the other route! Decision-making needs to consider the underlying concepts of resilience and then project these into the strategic and policy fields.

1.1 Agreement on distinct concepts

I propose that at least the following distinct concepts need to be considered.

- A ‘robust’ system, exposed to a horrendous overload will not suffer any irrevocable damage to the system and so the system will remain operational at its original level after the overload or natural disaster stimulus recedes.
- A system may be considered fragile if a single failure of a subsystem will inevitably cause a cascading failure.
- A system may be considered vulnerable, if every one of its subsystems is operating close to the capacity at which irrevocable damage may occur. In that situation, any assessment of the system will show that it is currently producing its designed output, but the assessment may fail to note that even a tiny additional event affecting even one tiny subsystem will almost certainly cause a cascading and irrevocable failure. This ‘tolerable disturbance’ concept has found its way into some of the seminal works on resilience.
- A system exhibiting “graceful degrade” can be expected to continue to offer exactly the same functional service (albeit slower etc) despite an event that causes permanent damage to a sub-system. A system exhibiting graceful degradation will include design redundancy, though the backup system is likely to have reduced performance. The key issue is absence of common mode failures between main and backup systems.
- A system with either stockpiles or design redundancy may be able to either draw down a stockpile, or retain functionality by invoking “System ‘B’” and after a single (System ’A’) failure, but following a failure of “system ‘A’”, the will have reduced capacity to withstand a second event and so following either the stockpile draw-down or the reversion to System ‘B’ cannot be considered as “resilient” until either stockpile is replenished or the failed “system-’A’ is replaced.
- It is possible to assess a system’s “Exposure” (Robertson 2017) as a measure of the number of points of failure: It is possible to identify systems that have high levels of exposure and hence warrant some priority for improvements. Equally importantly it is possible to observe whether any proposed change will increase or decrease the level of exposure.
- A ‘reliable’ system may simultaneously be quite deficient in robustness, highly vulnerable, and additionally ‘fragile’ (tiny failures will inevitably cause cascading and catastrophic failure) and may have absolutely no internal ability (resilience) to recover from a damaging event! Reliability only means that the failure has not happened often. Reliance upon ‘reliability’ is actually very dangerous, as it will tend to mask major and significant lacks of either robustness or resilience.
- When a subsystem (part of infrastructure) is actually broken (irreparably damaged) by some event (e.g. an earthquake), then after the cessation of the event (e.g. earthquake, or fire) the subsystem will remain broken. Although this is totally obvious, this situation is sharply distinguished from the reaction of a robust system that will simply revert to original functionality without intervention, following cessation of the disturbance. In the context of infrastructure, a broken subsystem absolutely will not ‘bounce back’, and restoration depends on external aid to replace/repair the broken item.

1.2 What should we seek?

Survivability is obviously critical, but I would argue that improved survivability (in the immediate aftermath of a natural disaster) is NOT what is under consideration. FENZ and NZDF capabilities are uniquely designed to

supply needs in this critical post-event timeframe, and the skills/resources for this specific function lie quite clearly within FENZ and NZDF scope – but these organisations cannot reasonably provide normal societal functioning beyond the short-term.

Long term recovery is also obviously important, but it could be claimed that all current systems are 'resilient' – i.e. given **enough** time and financial assistance, they are **all** theoretically capable of "bouncing back". This is perhaps stretching semantics, but I propose that it does let us focus on a better scoping of the goals of this consultation.

I submit that a useful interpretation of the objective of this work "...A resilient critical infrastructure system enables all New Zealanders, and the communities that they reside in, to participate in society and the economy with confidence that their essential needs will be met…" should emphasize the capability to continue all significant functions, after a major event, pending permanent reconstruction. I will use acronym MTR (Medium Term Resilience) – not necessarily expecting the phrase to become common parlance, but simply to make sure that the remainder of the submission is clear.

An illustration was provided in the aftermath of cyclone Gabrielle: cellphone towers' batteries were exhausted within hours, yet fibre-optic cables took weeks to repair! It is the intermediate (MTR) timeframes (between hours and months), where functional capacity is needed and where "resilience" can define its provision!

We should seek a situation where community functional needs are assured by the provision of robust systems, and systems that exhibit graceful degrade in the "MTR" timeframe.

2. Basis for defining infrastructure

I do not believe that there is a need to expend too much energy on this. For reasonable future, MTR requirements are:

1. Water supply, sewage removal and treatment. These issues can be addressed in an immediate post-event timeframe, but survivalist approaches may not assist genuine "bounce-back" in a medium-term post-event timeframe.
2. Energy. While liquid and solid fuel stockpiles can store very significant amounts of energy, we do not have a practical technology capable of storing enough electrical energy to supply enough power to run (for example) a domestic microwave or electric oven or charge an EV for more than some trivial period, and many essential services are dependent on 230V, 50Hz electricity supplies.
3. Communications. We may note that while communication (personal/commercial/medical), is fundamental to provision of other services, this is an infrastructural service that has become seriously 'exposed', as a result of reliance on measures of reliability rather than considerations of resilience.
4. Financial transactions. The capacity to pay for goods/services, and to accumulate payments is critical to a "bounce back". Since it is quite possible to separate this from communications, it is noted separately.
5. Physical movement of goods (roads/rail/drone etc etc); Any event in which "resilience" is significant will inevitably require the transport of goods: the means of transport is therefore a significant consideration in the provision of resilience.
6. Basic shelter. In the medium-term, and on the assumption that "resilience" is a consideration following some natural disaster, there is a need for at least a subset of buildings, designed and constructed to a standard that will provide a "place of refuge" for MTR, allowing citizens to have ongoing

accommodation for themselves and families, and also to continue essential business activities. This also requires consideration of what community size and distribution requires what level of facility.

The essential question (for categorising something as essential infrastructure) is the effect of MTR availability, and an observation that the capability cannot be reasonably stockpiled. The categorisation could reasonably also consider whether the current capability has required the dedicated effort over years and at national/international scale, in order to achieve current service levels.

In the longer term, we should consider criteria for removing a category from 'infrastructure' – for example, if large-scale electrical energy storage became practical, power transmission would no longer need to be considered as essential infrastructure.

3 Conclusion

3.1 Resilience standards

I would submit that NZ needs to develop agreement on resilience/robustness goals and hence standards, that are applicable across public and private infrastructure providers. These need to be agreed at national level, basic elements of agreement should include:

All essential infrastructure for all communities, should have an 'exposure' vulnerability below some agreed level and offer graceful degrade capability during the MTR timeframe.

All essential infrastructure for all communities, should be operationalised with the simple criterion that its "functional capability" must not be be able to lost from any single failure, and must continue to be available in the period until long-term solutions are implemented.

3.2 Application of standards across public/private

The aspirational capacity that all citizens can "participate in society and the economy with confidence that their essential needs..." is currently unachievable without the use of facilities that are currently only offered by private companies. Many of even the most basic facilities (capability to communicate, to aggregate and disperse (financial) resources and to access foodstuffs, fuel/energy and/or healthcare, are entirely controlled by private entities. It is entirely naive to consider that any private entity has any motive than the long-term return to its shareholders (which may involve some short term public good expenditure on non-profit activities and publicity). If there is an agreement that some functional capability is "critical infrastructure", then *ipso facto*, that capability is definitionally a "public good" and there is a need to support the "gap" between public good and private profit-maximisation.

If New Zealanders want to assure MTR access to some (infrastructure) capability, then there is a need to compel the means of access, and to find a practical means to fund these.

At present, courts have upheld the right of private entities to offer or with-hold services on their own terms: this does not align with the concept of inviolable rights of access to functional facilities that have been deemed to be public good critical infrastructure. The scope/extent of non-alignment is that the provision of backup and MTR services will generate costs but no returns to a private entity.

A practical assurance of critical infrastructural resilience therefore requires:

- A need to "deem" various functional capabilities as 'critical infrastructure" - including cases where these functional capabilities are currently provided by private entities. There is a commensurate need to define which groups of citizens can reasonably expect to have access to this infrastructure (it is not reasonable to expect a full suite of infrastructural services at each tramping hut in the Ruahine ranges).

- Need a clear specification of functional service level within a MTR period. The specification must itself be functional, and must be robust and must be applicable to whatever entity is providing the capability pre-event.
- The establishment of an independent body with a technical foundation sufficiently that is sufficiently strong to administer the provision of the agreed level of resilience.
- A funding model that is both practical and future-proof. Resilience is seldom available at zero cost and provision of resilience to an agreed level of public good does not align with normal commercial priorities. There is a need for a funding model that will ensure resilience now, and into the future.

No private entity can be forced to offer a service: the total of NZ citizenry may ultimately need to decide whether some functional need is a 'critical infrastructure', and how (if no private entity is prepared to provide it) the provision of such a critical infrastructural service is to be funded. This question is in the socio-political realm but does become relevant to the issue of this consultation.

Even where a critical infrastructure is provided by a private entity, I would submit that NZ should NOT allow any encroachment upon backup capabilities: Cash and even bullion should always remain as legal tender, and private entities should always be required to offer and accept such. Similarly, spectrum allocation to amateur radio and CB radio should never be revoked. I would further submit that NZ should never allow an assessment of reliability to confuse the need to provide robustness/resilience. The fact that a system has seldom broken, offers absolutely no assurance of MTR performance, must not divert/obscure the need for resilience measures.

3.3 Funding

There appear to me to be two cost models to cover resilience measures that become mandated:

- Private suppliers are required to develop resilience functionalities to a national standard, and are allowed to add the costs of these provisions to their current customer charges
- Private suppliers are required to develop resilience functionalities to a national standard, and are reimbursed from public funds for these measures.

Both models would obviously need independent audit provisions.

I submit that the second approach comes closest to the definitional goal that ".. all New Zealanders, and the communities that they reside in, to participate in society and the economy with confidence that their essential needs will be met".

Signed

Lindsay Robertson