Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018

Whilst the Security Legislation Amendment (Critical Infrastructure) Bill 2020 does introduce important modernisation to the Security of Critical Infrastructure Act 2018, some aspects may not have received sufficient consideration to adequately provide resilience to Australia's critical national infrastructure.

The WannaCry and NotPetya malware pandemics of 2017 illustrate the scope of global and national interconnectedness and inter-dependencies of critical infrastructures. Both of these malware variants affected multiple infrastructure sectors globally. Despite the NotPetya malware using the same exploits as WannaCry and propagating a month later, infrastructure operators and organisations were still unprepared. These incidents underscore two things: (1) the need for pro-active and predictive measures to inform preparedness and resilience; and, (2) that vulnerabilities in another nation's critical infrastructure may have negative effects on the economy, security, and critical infrastructure of another nation.

When considering cyber-attacks and international competition in the "grey zone" (see Sky News podcast "into the Grey Zone"), it is possible that multiple critical infrastructure sectors will be simultaneously eroded in conjunction with other stressors, such as fake news and compromised emergency communications in order to maximise confusion, panic, and instability. It is therefore imperative to give further consideration to infrastructure interdependencies, the consideration of emergency services and first responders as critical, and a holistic approach to national resilience to critical infrastructure incidents. The importance of national icons should also be acknowledged; whilst they may not provide critical services, their failure or destruction may have a profound psychological impact on the population. Buildings with large holding capacity may also prove useful as emergency shelters.

The latest research should be considered during the review process, to aid ascertaining the appropriateness of the Bill and Act, as well as the submissions. The following journals can be considered:

- *The Journal of Critical Infrastructure Protection*
- *The Journal of Information Warfare*
- *The Journal of Cyber Warfare and Terrorism*
- *The Journal of Law and Cyber Warfare*
- *Computers and Security*
- *The Journal of Cybersecurity*

The importance of multi-disciplinary perspectives cannot be overstated. Therefore, we suggest an advisory panel be constituted to advise and assist the Parliamentary Joint Committee on Intelligence and Security in these reviews. The panel should comprise of national and international experts with different perspectives (e.g. legal, social, economic, physical security, cyber security, strategy, terrorism) of critical infrastructure protection.

While there is a statement in the proposed Bill that critical infrastructure protection measures need to align to and respect human rights, further guidance can be provided in terms of the UN Group of Governmental Experts (GGE) 2015 report and the Global Commission on the Stability of Cyberspace's

2019 report (https://cyberstability.org/report/). These two sets of norms also specifically mention the protection of critical infrastructure, and provide guidance on some measures that can be highlighted in national efforts.

Please note, the opinions provided here are those of the respondents and not their affiliated organisations.

Kind regards,

Dr Brett van Niekerk, University of KwaZulu-Natal

Dr Trishana Ramluckan, Educor Holdings and University of KwaZulu-Natal