Benjamin Cronshaw

13th February 2022

Submission to the Inquiry into Critical Infrastructure

The Bill seeks to expand the number of features that are designated critical infrastructure, to a list of eleven sectors including higher education, food, healthcare, transport and others. This is an expansive view of Australian security, which is appropriate. There are many areas that are relevant for the security and wellbeing of the Australian people which, if disrupted, can cause great harm. I appreciate the range of existing and potential threats that are identified in page 2-3 of the explanatory memorandum and how these can and have impacted on Australia.

We have seen through the past couple of years that our daily lives can be seriously affected by disruptions, such as been caused by the pandemic. Disruption to supply chains and the fear generated by unpredictable events has also led periodically to panic buying, which disrupted access to grocery store goods and medical tests. There has also been a great strain in the healthcare system with hospital capacity being exceeded and exhaustion amongst healthcare workers.

Critical infrastructure can also be disrupted by natural disasters such as floods, cyclones and bushfires. This underpins the need to recognise what critical infrastructure is necessary for our security and the smooth operation of our society and, beyond that, what can harm or disrupt this infrastructure. With the impact of climate change in changing our landscape and leading to more extreme weather events and natural disasters, adapting our critical infrastructure and building resilience will be a critical task.

The Bill also identifies the threat from cyber-attacks. This is appropriate given the range of cyber-attacks that are happening around the world and making the news (with several notable examples in the United States targeting energy companies). There is a range of potential threats from private (commercially motivated) groups, terrorist groups or states. The threat from cyber-warfare, both private and state-sponsored, is likely to increase into the future. If Australia was to enter a war or conflict against an opponent with electronic-warfare capabilities, Australia could be open to cyber-attacks on our critical infrastructure. Cyber-attacks would also exacerbate vulnerabilities if Australia was already dealing with other events. A cyber-attack during a pandemic or natural disaster, for example, could disrupt our response and strain our capacity to respond to both threats at the same time. It is sensible to recognise the threat from cyber-attacks. This includes putting greater obligations on operators of critical infrastructure assets to prepare and secure themselves against electronic vulnerabilities.

In having an expansive view of security amongst many sectors that are important for the daily lives of Australians, and examining the threats to these sectors and how we should be prepared to secure them, I believe this Bill has an important role in our security planning. I support the Bill.

Kind Regards,
Benjamin Cronshaw.