Re: Statutory Review of the Security of Critical Infrastructure Act 2018

Author: Paul Wilkins

Date: 4 February 2021

Contents

Introduction

The author welcomes this opportunity to contribute advice to the PJCIS in efforts to formulate national policy for telecommunications security, and to make the following points:

- Telecommunication physical assets are not unamenable to being brought under the umbrella of the "*Security of Critical Infrastructure Act 2018".*
- Critical telecommunications services require cybersecurity mechanisms. Cybersecurity is a separate domain from traditional utilities security, and requires its own specific risk management framework.
- The need to formulate a "National Carriage Security Profile" to create a uniform baseline for the protection of critical telecommunications infrastructure and services.
- The need to recognise a "National Carriage Boundary" as critical infrastructure, as the demarcation zone between endogenous and exogenous traffic flows.

Protection of Telecommunications Physical Assets

As concerns the security of national telecommunications, and whether "whether it would be appropriate to have a unified scheme that covers all infrastructure assets (including telecommunication assets)", those unfamiliar with IT security should be apprised that physical security and cybersecurity are disparate entities not amenable to being brought

within a common paradigm. While one could bring the protection of physical telecommunications assets (premises and hardware) under the umbrella of traditional utilities which rely primariliy on physical protection mechanisms, this would result in difficulties around demarcation and responsibility. For instance, access mechanisms for data centres perform a double duty, where they protect physical infrastructure from physical threats, but have additional policy mechanisms to protect against cyberattacks which rely on a physical vector. It is often the case that in the washup after an attack, it's identified that failure to prevent the threat is the result of the vector slipping between gaps in demarcated responsibilities.

The "Security of Critical Infrastructure Act 2018" represents a culmination of efforts to secure traditional utilities. Security measures primarily rest upon traditional security measures to protect physical infrastructure. There ought to be government mechanisms to ensure the protection of the physical infrastructure of critical telecommunications infrastructure (premises and hardware), and such mechanisms could be brought under the umbrella of the "Security of Critical Infrastructure Act 2018". It's arguable this is not the best fit, and that they should be brought under the telecommunications cybersecurity umbrella. Either you put all physical security under the one umbrella, or you put all telecommunications security under the one umbrella. What is more important is that there are risk mechanisms for telecommunications physical infrastructure, and there are good lines of communication to both the telecommunications cybersecurity umbrella and traditional utilities security umbrella.

Physical Security and Cybersecurity are Distinct Domains

Cybersecurity is the protection of the manifold internetworked information planes that exist above the physical infrastructure (premises and hardware). It should be immediate apparent that this distinction means that the cybersecurity of national telecommunications cannot be accommodated within a security framework designed primarily to address the physical security needs of traditional utilities. Management and operation of cybersecurity is a specialist domain, and is unamenable to being accommodated within a framework designed to address the risks of traditional utilities: predominantly physical threats to physical infrastructure.

- Cyber threats to Internetworking infrastructure are virtual in nature, meaning they cannot be physically isolated. Threat vectors to Internetworking infrastructure can originate from anywhere in the internet. Furthermore, VPN, Dark Nets etc. guarantee that the source and authors of these threats are difficult to isolate.

- Traditional utilities are not subject to the multiplication of risk arising from attacking multiple targets simultaneously, where all targets share a common vulnerability. Where targets share a vulnerability to a single threat vector, the sum

vulnerability is the sum of these multiple targets. This multiplication of vulnerability can emerge in many forms:

- Shared software vulnerability – eg: A virus attack where many enterprises share the same vulnerability.
- Threats to carriage infrastructure – such as bulk flow saturation, BGP or DNS denial of service attacks that take down or degrade national carriage infrastructure or critical services.
- Saturation level traffic flooding that degrades the ability of a shared communications link to carry traffic.
- Threats to Public Key Infrastructure – where multiple enterprises rely on specific certificate authorities for authentication and/or authorisation of agents and/or verification of software images.
- Internet site impersonation/hijacking, where an internet site that provides an essential service is coopted, either to enable a subsequent attack (such as by stealing credentials), or as an attack in its own right (ecommerce fraud, theft of intellectual property, etc)

Consolidation of Telecommunications Cybersecurity Regulation

The PJCIS is not unfamiliar with advice that national cybersecurity policy needs a consolidated approach. The response to this advice to date has been disappointing, where against advice, we have seen the imposition of heterogenous and poorly coordinated regulatory requirements, notably regarding the Interception and Access Act 2015 and the Assistance and Access Act 2018.

In submissions to these enquiries, the point was made in many submissions that a consolidated framework for national telecommunications cybersecurity policy is needed to ensure coordination of efforts, maximised returns in terms of security for time and resources invested, and the preferred path to ensuring obligations under the regulatory regime can be most easily understood.

Consider the following examples:

The Interception and Access Act 2015 grants a plethora of agencies the power to request metadata from carriers, with consequence confusion amongst carriers as to the extent of legitimate authority vis a vis a particular agency's requests, in the face of competing priorities including corporate governance and legislative obligations, including privacy protections and due diligence. It is the case that due to the plethora of requesting agencies, which are not all themselves experts in the exercise of the enabling legislation, or best understand the most efficient methods to extract the pertinent information of most benefit to their investigations. This framework imposes obligations on each carrier to establish working process with each new agency they engage with, which is not an efficient means of ensuring engagement between government and industry. Preferable would be

engagement with a single agency which well understands the enabling legislation and has established processes for engaging industry.

The Telecommunications Sector Security Reforms, introduced with the "Telecommunication and Other Legislation Act 2017", introduced an obligation for carriers to "do their best" to protect telecommunications networks. The clear ambiguity and arbitrariness of a "do their best" test guarantees difficulty in guiding the development of national telecommunications security, where there is no conformity of policy, processes, or architecture.

The "Security of Critical Infrastructure Act 2018" grants the Attorney General the power to issue Technical Capability Notices, and to a plethora of agencies the power to issue Technical Assistance Notice. There appears to have been little consideration during the policy formulation of this framework of maintenance of changes imposed by individual agencies, or coordination of efforts across agencies. This guarantees that over time there will be complications arising from heterogenous and incompatible requests. Furthermore, the failure to establish a common framework and process flow for servicing metadata requests will result in inefficiencies. It would have been preferable for a single government agency to have been tasked with industry engagement for metadata requests, and this agency then to act as a clearing house across investigating agencies.

It continues to be the case that under S317A of the Telecommunications Act 1997, the Attorney General has the power to issue Technical Capability Notices with the effect of compelling carriage providers to provide metadata streams of metadata collected under 187A of the "Telecommunications (Interception and Access) Act 1979". There should be concern where even at the level of legislative instrument, the overlap of separate legislation gives rise to such unanticipated consequences, due to the lack of a uniform framework for policy development.

A National Carriage Security Profile

In both policy formulation, and the subsequent derivative legislation, there ought to be made an explicit distinction between endogenous carriage (carriage within national borders) and exogenous carriage (carriage that crosses international boundaries), and recognition/definition of a "National Carriage Boundary" to serve as a demarcation zone between endogenous and exogenous carriage networks, and for the application at the demarcation zone, of a standard and well defined National Carriage Security Profile on exogenous traffic flows.

The explicit recognition of this distinction would then be able to inform policy. The first consequence of such a recognition would be to create an architectural separation between endogenous and exogenous carriage, where exogenous carriage is explicitly recognised as having no security posture, while endogenous carriage has a recognisable and uniform security profile, defined by policy and legislative instruments. There should be statutory obligations on carriers to ensure that exogenous traffic flows align with the National Carriage Security Profile.

The distinction of carriage as either endogenous or exogenous, would then establish a demarcation zone at the national boundary, where national carriage security policy is imposed on exogenous traffic passing into or out of the national borders. This would facilitate valuable outcomes, including security at scale for national carriage networks and essential network services, the imposition of national jurisdiction on exogenous traffic flows, efficiencies of scale in addressing existential threats to the national carriage infrastructure, and creating the necessary framework, architecture, policies, and processes for cooperation and collaboration amongst exogenous carriers, and between them and government/security agencies.

Despite the merits of asking that carriers do "their best" to protect national networks as provided under Sections 313(1A) and (2A) of the Act, "their best" is subject to arbitrary definition and the individual interpretation of each carrier, preventing the development of uniform standards, architecture and processes. This is recognisable, for instance, in the "Clean Pipes" initiative, where some carriers are taking it on themselves because there is a lack of national policy. But the development of such initiatives is subject to the brand alignment of enterprise carriers vying for competitive advantage. Cooperation between carriers on the basis of a "best effort" obligation, cannot be effective or scalable. What is required is national policy and standardised architecture and processes to create a baseline security profile that applies across the national carriage network, and this requires the imposition of a national security posture at the endogenous/exogenous carriage interface, the "National Carriage Boundary".

Furthermore, it may be actually impracticable under the present framework for exogenous carriers to mitigate certain risks to infrastructure and services, even if they were of a mind to address the risk. Owing to Australia's rather unique geography as an island continent, the "National Carriage Boundary" is essentially an aggregate network of submarine cables. Due to existing commercial arrangements, carriers may have little architectural or operational control of the distal ends of submarine cables, operated and maintained by commercial partners, and because these locations are offshore, not subject to Australian jurisdiction. Recognition of a "National Carriage Boundary" and the definition of a National Carriage Security Profile would be able to inform future commercial arrangements and architectural development of distal submarine cable head ends.

The National Carriage Boundary is Critical Infrastructure

Once given recognition of the National Carriage Boundary, policy should address potential threats to this essential infrastructure. For instance, one possible disaster scenario of concern to those shaping national carriage security, would be the failure of significant domestic cloud data centre(s), where an aggregate of service providers have a primary location in an Australian cloud data centre, but they have all opted for an offshore backup data centre location. A failure of the domestic primary data centre would give rise to an en mass relocation of Australian based services to offshore data centres, resulting in significant additional bulk traffic flows needing to be carried across the National Carriage Boundary. If these links were to saturate, national carriage services would be significantly impacted. Responsibility for addressing such a scenario rests squarely with government, where no exogenous carrier acting on their own initiative is capable of mitigating such a risk, even if they were of a mind to. Furthermore, cooperation amongst exogenous carriers is better able to spread the risk, but only where mechanisms for coordinated cooperation exist.

One approach might be for the Critical Infrastructure Centre to act as a point of coordination between exogenous carriers and the security agencies to ensure a consistent security profile applies at the National Carriage Boundary.

Extant Gaps in National Carriage Security Infrastructure

	Present State	Goal Architecture
National Carriage Boundary	No clear demarcation between exogenous and endogenous carriage networks	Establishment of a National Carriage Boundary, to serve as demarcation between endogenous and exogenous traffic
Standards	Best effort (per 313(1A)) as interpreted by carrier – arbitrary, heterogeneous, and unscalable	A single National Carriage Security Profile, to be adopted across all exogenous carriers, to be applied to exogenous traffic flows
Jurisdiction	No clear demarcation between exogenous and endogenous carriage	Imposition of sovereign jurisdiction on exogenous traffic flows via legislative instruments at the National Carriage Boundary
Architecture	Ad hoc across carriers and unscalable	Standardised baseline architecture for the National Carriage Boundary
Process	Ad hoc across carriers and unscalable	Established standardised mechanisms for exogenous carrier engagement
Cooperation	Ad hoc across carriers and unscalable	Standardised processes for intercarrier cooperation and liason with security services Standardised processes for the evolution of the National Carriage Boundary architecture
Essential Network Services - Bulk Carriage (protection against DDoS etc) - BGP routing - Domain Name Service (DNS) - Public Key infrastructure - Cloud Services (compute and offline storage)	Heterogeneous enterprise level protection Unscalable No specific mechanisms for protection of essential network services from exogenous sources	Established architecture, policy, and standardised processes for protection of essential network services at the National Carriage Boundary
National Carriage Boundary bulk flow capacity	Ad hoc across carriers Carrier security mechanisms don't address wider threats to the National Carriage Boundary	Established architecture, policy, and standardised processes for risk management of threats to bulk carriage across National Carriage Boundary