A National Telecommunications Security Posture

Author: Paul Wilkins

Date: 24 October 2024, V: 1.9

Initial Release: 27 April 2021

Contents

Architecture of Government's "Cyber Security Strategy 2023-2030" Wants Vision

The Department of Home Affairs has published the "Cyber Security Strategy 2023-2030"[1]. Firstly, it's not clear where this document purports to speak for whole of government policy regarding telecommunications, when this properly falls within the purview of S8 of the Australian Communications and Media Authority Act 2005, and as such policy formulation for telecommunications is the responsibility of the Department of Infrastructure, Transport, Regional Development, Communications and the Arts. This is a big deal. The brief of Infrastructure and Communications is nation building. The brief of Home Affairs is enforcement. It's the difference between bolting the door after the horse, and building better barn doors.

While Department of Home Affairs has conducted a consultation process in the formation of the Cyber Security Strategy within the ambit of security for systems of national significance, it's not clear where and to what extent Department of Communications has engaged with this process as pertains development of telecommunications policy.

[1] Department of Home Affairs: https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf

The document addresses threats and strategies to address those threats. However, lacking from this document is the framework that would provide an overarching architecture that would inform a national policy direction for the mitigation of cyber threats to the national telecommunications network. Where the Cyber Security Strategy is the guiding justification for a $1.67bn investment of public dollars, it's important that the strategy is correct, and that all options are considered to get best return on investment in terms of protecting national telecommunications. It's important to note where the Security Critical Infrastructure Act 2018, intended to impart the legislative momentum to the strategy, would appear to apply only to telecommunications physical assets[2], and so arguably cannot lawfully enforce a cyber strategy for the protection of the manifold information planes that exist above the physical infrastructure.

There exists a very great once in a lifetime opportunity that would lift the security of all boats, across the Australian telecommunications network. It's a basic principle of enterprise network security design, that threats should be blocked as close as possible to the origin of the threat. The premise applies no less in the national context. Australia's cyber security strategy should aim, where possible, to mitigate threats as close as possible to the source of the threat.

Australia's geography as an island continent, means that the national carriage network exists as a network island, where international interconnects are principally submarine cables. This "National Carriage Boundary" is a natural demilitarised zone, and could act as a point of enforcement of a National Telecommunications Security Posture, where many threats to the national telecommunications infrastructure could be blocked, providing a uniform level of baseline security across the national telecommunications network.

[2] Security of Critical Infrastructure Act 2018 S9 definition of "critical infrastructure" applies to "assets", not services.

Serendipitously, Australia has moved all wholesale supply of domestic broadband internet to the NBN, at a cost burden to the taxpayer of $51bn. This infrastructure could be similarly leveraged to act as a DMZ for policy enforcement for all domestic traffic.

The establishment of the National Carriage Boundary as a point of policy enforcement 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

The principal purpose of the National Telecommunications Security Posture would be to block bulk flow traffic attacks ie. DDoS (distributed denial of service). The principal use case would be to identify through statistical analysis of traffic patterns at the IP transport layer, and through heuristics of source/destination address and port information, identify bulk flow traffic attacks. Attacks identified would then generate an advice to the relevant carrier for corrective action (which can be automated). Once these network touch points were established, the architecture could be leveraged to protect against other attack types. Inspection of TCP headers would allow heuristics to extend to identification of SYN flow attacks. The architecture could also be leverages for the protection of critical network services, BGP and DNS for example.

The end result is that with the right architecture, a National Carriage Security Posture could be applied across the national telecommunications network, which would provide a baseline level of security across the national telecommunications network. Identifying and eliminating Transport layer network attacks at the point of ingress to the national telecommunications network, would materially improve baseline security across the national telecommunications infrastructure. It would scale, where with these threats eliminated from the national network, enterprises and governments can direct valuable security resources to address network threats at a more granular level.

There exists a once in a lifetime opportunity to leverage Australia's geography, and the $51bn investment in wholesale NBN broadband, to institute a national telecommunications security posture, that would protect against DDoS traffic flooding, and could be leveraged to protect against other telecommunications based attacks, including command and control bot networks and ransomware attacks. Essentially, the national telecommunications network would be protected by having the National Carriage Boundary, and the NBN, perform the functions of a DMZ (demilitarised zone).

The National Carriage Boundary as a Demilitarised Zone

An architecturally sound approach to the development of national telecommunications security policy, should make explicit distinction between endogenous carriage (carriage within national borders) and exogenous carriage (carriage that crosses international boundaries). This would give recognition to a "National Carriage Boundary" 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 Posture on exogenous traffic flows.

The explicit recognition of this distinction would then be able to inform policy. Recognition of architectural separation between endogenous and exogenous carriage would flow through to inform policy development, where exogenous carriage is explicitly recognised as having no security posture, while endogenous carriage would have a baseline 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 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.

While carriers have obligations under sections 313(1A) and (2A) of the Telecommunications Act 1997, to do “their best”, this is at best an arbitrary standard, and the lack of definition allows for individual interpretation by each carrier, preventing the development of uniform standards, architecture and processes, and provides no impetus to establish the uniform security profile that would both lift all boats, and provide the necessary mechanisms to protect Australia’s National Carriage Boundary.

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 legislative and commercial arrangements and architectural development of distal submarine cable head ends.

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 in aggregate, 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, potentially magnifying the impact of an ongoing cyber attack against the national carriage infrastructure. 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.

The institution of a national telecommunications security posture also alleviates the difficulty for carriers, where for the regime proposed under the Security Critical Infrastructure) Act 2018 to be effective, carriers would need to associate their network assets and services with the respective systems of national significance which they service. Where there is a baseline national telecommunications security posture, there is no such obligation, where the raised security profile “lifts all boats” across the national telecommunications infrastructure.

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) - Email (anti spam/phishing) - BGP routing - Domain Name Service (DNS) - Public Key infrastructure	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 Stochastic anomaly based prevention/detection Signature based prevention/detection

- Cloud Services (compute and offline storage)		
Essential PSTN & SMS Services	Ambiguous "Telecommunications Act 1997", requirement that carriers must do their best to "prevent telecommunications networks and facilities from being used to commit offences"	Established architecture, policy, and standardised processes for protection of essential telephony services at the National Carriage Boundary National Telephony Carriage standards Stochastic anomaly based prevention/detection Signature based prevention/detection
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
Interdiction of criminal activity	Heterogeneous architecture, policy, and enforcement processes Inability to discriminate endogenous/exogenous traffic/activity	Established architecture, policy, and standardised processes for enforcement of Australian jurisdiction More granular specificity in enforcement actions

The NBN as a Demilitarised Zone

DDoS (and other traffic flood type attacks) at source can conceivably originate from 3 sources:

1. Sources outside the Australian jurisdiction (ie outside the National Carriage Boundary)
2. Domestic Non NBN sources – high bandwidth, commercial services
3. Domestic NBN sources – low bandwidth consumer services

Blocking DDoS attacks of type (1) at the National Carriage Boundary is scalable, and ensures DDoS protection not for particularly prioritised services, but ensures a level of protection against traffic flooding across the national telecommunications infrastructure. Indeed, the same effect would ensue should the Secretary, issue to exogenous carriers (identified as systems of national significance), a S30DJ(2)(c)[3] direction to ensure continuity of service for the national telecommunications infrastructure.

DDoS attacks of type (2) originating from commercially significant services, would presume the service customer to be a responsible operator, and to have mature security procedures; and in the event should they be found to be producing significant DDoS traffic, there are likely mature processes for eliminating the source. Where the generation of DDoS is found to be not inadvertent, but deliberate, criminal prosecution serves as sufficient disincentive, under the existing s474.17 of the Criminal Code Act 1995, use of a carriage service to harass. Consequently type (2) sources of DDoS and other traffic flooding attacks are not going to present as a significant volume of traffic sources.

DDoS attacks of type (3) from low bandwidth consumer services have a particular profile within the Australian context, where all domestic traffic transits a wholesale NBN carriage service. Australia has invested $51bn in NBN infrastructure, and it would appear to represent a poor return on this significant investment if the opportunity is missed to leverage this infrastructure to protect national telecommunications from

[3] Security Legislation Amendment (Critical Infrastructure) Bill 2020

DDoS and other domestic traffic flooding scenarios. A more considered framework would ensure mechanisms, both technical and process, to ensure cooperation between ISPs and NBN to identify DDoS sources and block this traffic. This system could be entirely automated, for an NBN advisory that a customer is originating flooding traffic to pass to the customer's ISP, and for the ISP to throttle their traffic until the attack ceases. The effort and resources required would be a fraction of what will be required for systems of national significance to each individually procure DDoS protection. The end result vastly superior, where the national telecommunications infrastructure has blanket protection against flooding attacks from domestic sources.

Architecture for Security of Telecommunications under the Australian Cyber Security Strategy 2023 framework, versus security under the two heads of the National Carriage Boundary, and the NBN

	Cyber Security Strategy 2023-2030 Framework	Architectural and Security Regulation on 2 Heads – National Carriage Boundary and NBN
Scalability	"All eggs in one basket" Consolidates DDoS service, making delivery of critical telecommunications services contingent on Tier 2 services DDoS directed procurement under S30DJ(2)(c) for Systems of National Significance	Distributed and scalable DDoS held at National Carriage Boundary shields national telecommunications DDoS held at NBN wholesale scales across ISPs retailers
Reliability	Creates framework for consolidation of DDoS services with Tier 2 providers, posing additional failure mechanisms for critical infrastructure	Services delivered through decentralised (scalable) Tier 1 service providers
Architecture	Centralisation under Tier 2 DDoS service providers counter to basic internet premise of reliability through a distributed network	Consistent with internet distributed network philosophy, natural positioning due to Australian continental geography, and national $51bn investment in NBN
Judicial Enforcement	NA	Provides touch points for law enforcement action
Security	Saturation of DDoS service providers can cascade to impact multiple critical infrastructure providers and services	Institutes a baseline security posture for national telecommunications security Could be leveraged to protect against other attacks, including bot networks and ransomware

Value for money	Drives investment in sub standard architecture	Investment in National Carriage Boundary leverages to protect all Australian telecommunications Leverages national $51bn investment in NBN

Obligation of Government to Direct Architecture for the Security of National Carriage

It presents as an open question why this architecture should not be instituted under the obligations of S5, S311, and S313 of the Telecommunications Act 1997, that carriers must do their best to "prevent telecommunications networks and facilities from being used to commit offences", and "do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access."

- S5 The ACMA, carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences.[4]

- S311 Carriers and carriage service providers have a duty to do their best to protect telecommunications networks and facilities from unauthorised interference, or unauthorised access, for the purposes of security. [5]

- S313 Obligations of carriers and carriage service providers[6]

  (1) A carrier or carriage service provider must, in connection with:
  (a) the operation by the carrier or provider of telecommunications networks or facilities; or
  (b) the supply by the carrier or provider of carriage services;
  do the carrier's best or the provider's best to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the States and Territories.

  (1A) For the purposes of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), a carrier or carriage service provider must, in connection with:
  (a) the operation by the carrier or provider of telecommunications networks or facilities; or
  (b) the supply by the carrier or provider of carriage services;
  do the carrier's best or the provider's best to protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access to ensure:

[4] Telecommunications Act 1997 S5
[5] Telecommunications Act 1997 S311
[6] Telecommunications Act 1997 S313

> (c) the confidentiality of communications carried on, and of information contained on, telecommunications networks or facilities; and
>
> **(d) the availability and integrity of telecommunications networks and facilities.**
>
> (2A) For the purposes of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), a carriage service intermediary must do the intermediary's best to protect telecommunications networks and facilities used to supply the carriage service referred to in subsection 87(5) from unauthorised interference or unauthorised access to ensure:
>
> (a) the confidentiality of communications carried on, and of information contained on, telecommunications networks or facilities; and
>
> **(b) the availability and integrity of telecommunications networks and facilities.**

It needs to be emphasised, however, that there is currently no framework against which the criteria of "do their best" can be measured. This can be viewed as a lapse in diligence by the ACMA, of obligations under the Telecommunications Act 1997:

> The ACMA, carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences.

The ACMA has both a mandate, and a public interest obligation, under the relevant Telecommunications Act 1997[7] provisions to develop a relevant industry code:

- S 113 (3)(pc) the ACMA has a duty to develop relevant industry codes for the characteristics of carriage services supplied using optical fibre lines.
- S 113 (3) (pd) the ACMA has a duty to develop relevant industry codes for performance requirements to be met by carriage services supplied using optical fibre lines;
- S 115 (5) that the ACMA has a duty to develop relevant industry codes for:
    - optical fibre lines; or
    - facilities used, or for use, in or in connection with optical fibre lines;

[7] Telecommunications Act 1997
S113 (3)(pc) "the characteristics of carriage services supplied using optical fibre lines;"

S 113 (3)(pd) "performance requirements to be met by carriage services supplied using optical fibre lines;"

S115 (5) The rule in subsection (1) does not apply to an industry code or an industry standard to the extent (if any) to which compliance with the code or standard is likely to have the effect (whether direct or indirect) of requiring:

(a) optical fibre lines; or
(b) facilities used, or for use, in or in connection with optical fibre lines;

to:

(c) have particular design features; or
(d) meet particular performance requirements.

Hence the ACMA have a policy, if not regulatory obligation, to ensure the existence of a governance and policy framework, and a relevant industry code, that can hold carriers to account for their S5 obligations to “do their best” to protect the national telecommunications infrastructure from denial of service attacks. Otherwise, the S5 obligation is both subject to arbitrary interpretation, and has no compliance mechanisms, leaving the S5 stipulation dangerous in that it creates the perception of risk management provisions which do not, in fact, exist.