Re: Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 – Supplementary #2

Author: Paul Wilkins

Date: 14 April 2021

Supplementary #2

Contents

Cyber Security Incident under S12M should extend to Telecommunications Services 1
Recognition of a Telecommunications Service Cyber Security Incident (proposed) S12M (e) 2
Definition of Systems of National Significance Under 52B 4
Procurement of DDoS Services per 30DJ(2)(c) 4
Responsibility of NBN vis a vis DDoS of Systems of National Significance 6
Responsibility of Governmend to Direct National Telecommunications Achitecture 9

Cyber Security Incident under S12M should extend to Telecommunications Services

Per the drafting of S12M, of the "Security Legislation Amendment (Critical Infrastructure) Bill 2020", the definition of "cyber security incident", subsections (a) through (d) are specific to affected computers, computer data and/or computer programs. There is apparent intent that the definition should extend to cyber security incidents of telecommunications services, but the current drafting leaves it vague as to whether S512M can in fact apply to telecommunications services. Interruption of telecommunications services (themselves critical infrastructure), will have significant impacts for essential infrastructure and systems of national significance, so there is a clear need for clarity as to the obligations that apply to telecommunications services regarding cyber security incidents.

The closest the current draft comes to addressing impairment/interruption of a telecommunications service under S12M would be subsections (c) and (d).

> (c) unauthorised impairment of electronic communication **to or from a computer**;
>
> (d) unauthorised impairment of the availability, reliability, security or operation of: (i) a **computer**; or (ii) **computer data**; or (iii) a **computer program**.

The problem lying, where recognition of a telecommunications service cyber security incident, is contingent on the same cyber security incident extending to an identifiable end use computing device. And even then, where the telecommunications service cyber security incident can identify an end use compute device affected by the same security incident, it's not clear that where the end use compute device is not within the sphere of responsibility of the carriage provider, that the end use compute device cybersecurity incident can be extended to apply to the telecommunications service, or that the carriage provider can be held to account for a cyber security incident that extends beyond their sphere of responsibility. So in instances of a telecommunications service cyber security incident, where either an impacted end use compute device cannot be identified, or is not within the sphere of responsibility of the carriage provider, it's not apparent how the definition of S12M can apply. Consequently, to the author's reading, impairment/interruption of essential telecommunications services falls outside the scope of the S12M definition.

The current draft consequently, has limited application to computer networks, only applying where both the computer and network are within the sphere of responsibility of a single party. In such a situation (typical for tail end computer networks), there is no difficulty of demarcated responsibility, where responsibility for both the network operation or the computer's operation lies with the same party.

Recognition of a Telecommunications Service Cyber Security Incident (proposed) S12M (e)

An additional subclause 12M(e) is recommended, that would afford explicit definition of a cyber security incident as pertains to a telecommunications device or service. Such a clause would need to meet the following conditions:

- The definition should apply to both a telecommunications device, and its upstream neighbour device
- The definition should apply to both an impacted telecommunications device and/or an impacted telecommunications service
- Recognition of service impairment/interruption to the data plane of a telecommunications device or service
- Recognition of service impairment/interruption to the control plane of a telecommunications device or service
- Applies across all telecommunications switched network technologies – circuit switched, cell switched, packet switched.
- A quantitative measure of service degradation that constitutes a cyber security incident
- Recognition that the telecommunications device is "in service"

The definition needs to apply to both a telecommunications device, and its upstream neighbour device, so that a cyber security incident that affects a telecommunications link is identified, without being explicit as to the A or B end device of the link. Consider a carrier that owns and operates both the point to point link and the downstream B end, where a DDoS is saturating the buffers of the upstream A device. There is impairment of service delivery at the B end, but the service impairment is invisible to the B device. The asset with the problem, the upstream A router with the buffer overflow, is outside the immediate sphere of responsibility of the carrier. In such a scenario, there is no device or service within the sphere of responsibility of the carriage provider that is not performing as intended. Under the draft Bill, the carrier has no obligations to recognise a cyber security incident. It should be required that the carrier recognises that the service is subject to a cyber security incident due to the impairment of the service's upstream peer, and should have reporting and other obligations as pertains the resolution of the incident in cooperation with the operator of the upstream A device.

A quantitative measure of service degradation is required, because carrier switched services rely on the statistical multiplexing of stochastic processes to ensure performant levels of service. Service delivery of stochastic processes will significantly degrade towards the upper end of resource utilisation[1], and it's not required that a resource be utterly exhausted before there is significant impact on service delivery. Less than 10% capacity is considered (by the author) as an acceptable compromise measure, between resource exhaustion (0 % spare capacity), and normal business practice where resource utilisation of stochastic processes are typically aimed to provision 30% spare capacity.

The clause should be explicit that the device is "in service". A device should be able to be taken out of service for the purposes of maintenance or as part of automated redundancy mechanisms, provided dependent telecommunications services are not impacted.

Recommended additional clause 512M (e)

> **512M (e) A telecommunications service, or an active telecommunications device, or an active upstream peer telecommunications device, experiences interruption of service, inability to deliver service, or has less than ten percent spare capacity of a service critical resource for a period exceeding 30 seconds.**

[1] A consequence of the maths of queue theory, where the likelihood of a service interruption climbs rapidly as a queue approaches capacity. The need to ensure spare queue capacity applies to all queued (hence switched) electronic communications, and so applies regardless of the deployed technology: circuit/cell/or packet switched.

Definition of Systems of National Significance Under 52B

A further obstacle to the recognition of a cyber security incident of essential telecommunications services results from the S52B definition of systems of national significance.

> 52B Declaration of systems of national significance by the Minister
>
> (1) The Minister may, in writing, declare a particular **asset** to be a system of national significance if:
>
> (a) the **asset** is a critical infrastructure asset; and

S5 definition of a telecommunications system "asset" would be:

> asset includes:
>
> (b) a network; and
>
> (i) any other thing.

As such, the purview of network assets is limited to physical infrastructure, and does not extend to the manifold virtual data/control/management planes that exist above the physical asset. For the Bill to afford full coverage of threats to essential telecommunications services, the definition of system of national significance needs to extend beyond the physical "asset" to address threats to those essential telecommunications services that are delivered over, or rely upon, those assets.

Procurement of DDoS Services per 30DJ(2)(c)

Section 30D(2)(c) grants the Secretary powers to compel customer procurement of telecommunications services under direction, and subsequently to accept responsibility for the level of service delivered by the carrier. This power on examination would extend to include the power to direct procurement of DDoS and other firewalling/feed filtering services.

> (2) The Secretary may, by written notice given to the entity, require the entity to:
>
> (c) take all reasonable steps to ensure that the computer is continuously supplied with an internet carriage service that enables the computer program to function.

This places a disproportionate onus of "caveat emptor" responsibility of ensuring service continuity on the service customer, without recognising that the carriage provider has responsibilities to ensure reliability of service, and that a customer has little agency to control the level of service provided.

The agency to establish structural integrity and security of the national telecommunications network lies not with customers, but with carriers and government.

A further deficiency in the 30D(2)(c) drafting, is where its scope is narrower than telecommunications services, and restricts itself to only "internet carriage service". And so, overlooks telecommunications that are not internet/packet based, which is the case for the critically important instance of call capacity of telephone exchanges. There will be other use cases, of critical infrastructure relying on telephone call routing for electronic communications, including telemetry and out of band management, both critical to the resolution of cyber security incidents.

Where a carrier fails to deliver a telecommunications service, it's neither feasible nor just to make the downstream users of the service solely responsible for ensuring continuous service delivery. It's fair that the customer be expected to exercise due diligence in procurement of the service. But in practice, there are structural obstacles for a customer to:

- Make alterations to a carrier's standard offering
- Ensure through contractual arrangements that a telecommunications service is fit for their specific purpose
- Ensure through contractual arrangements continuous delivery of a telecommunications service

Where the service fails, responsibility cannot fairly be sheeted home to the customer for procuring a service that's initially assessed as fit for purpose, but in practice, fails to meet reasonable expectations of continuous service. Under the current framework, the onus of "Caveat Emptor" rests squarely with the customer. This approach is ill advised and naïve. Firstly, to the degree that critical infrastructure providers are assumed not to have provisioned their telecommunications procurements responsibly, and that government direction will produce better outcomes looks like hubris. But there is a further serious difficulty, where the proposed regime presents to have a solution to structural inadequacies in the national telecommunications infrastructure, and that poor service delivery or interruption to national telecommunications infrastructure, can be resolved on a case by case basis by customers exercising better choice. This framework cannot deliver a solution where the customer has responsibility, but no agency. Which is to say, customer choice cannot address weakness in a carrier's network structural architecture, or weakness in the national telecommunications network architecture more generally. Responsibility for the integrity of the national telecommunications network, should rest with the aggregate of carriers, shaped by appropriate government regulation.

What is missing from the Bill is necessary consideration of governance mechanisms to hold carriers to account for the delivery of telecommunications services for systems of national significance, and the architectural direction that would address threats to the structure of the national telecommunications network.

Responsibility of NBN vis a vis DDoS of Systems of National Significance

Reliance on S30D(2)(c) direction to address DDoS threats institutes a framework where remedy is sort against DDoS attacks at the destination. Placing the onus on the carriage destination to protect against DDoS is not going to be cost effective, effective in protecting systems of national significance against DDoS, or scalable. Nor is such an architecture easily leveraged to protect against other threats.

A more considered and scalable approach is to impose restrictions on DDoS (and other traffic flood type attacks) at source. These can conceivably originate from 3 sources:

1. Sources outside the Australian jurisdiction (ie outside the National Carriage Boundary[2])
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 S30D(2)(c) 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 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

[2] See author's initial submission

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.

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".

- S5 The ACMA, carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences.[3]
- 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. [4]

- S313 Obligations of carriers and carriage service providers

  (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.[5]

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

Delivery of Telecommunications to SoNS under the Bill's framework, versus security under the two heads of the National Carriage Boundary, and the NBN

	Bill's Framework – Service Procurement under 30DJ(2)(c) direction	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	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

Responsibility of Governmend to Direct National Telecommunications Achitecture

There is a fundamental principle of network security architecture, that threats should be identified and mitigated as close as possible to the source. This is a basic principle of enterprise network architecture, and is no less relevant in the context of the national telecommunications infrastructure. Best practice would be for the government to institute protection mechanisms for DDoS and other bulk traffic flooding attacks, at the primary points of ingress to the national telecommunications network: the National Carriage Boundary, and the NBN. Such an architecture could be leveraged to address other types of attacks, such as command and control bot networks.

The institution of a national telecommunications security posture also alleviates the difficulty for carriers, where for the regime under the Bill 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.

In conclusion, there is 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).

Recommendation:

For the PJCIS to refer the Bill back to Department of Home Affairs, for consideration of an alternate framework for the protection of the telecommunications services of systems of national significance, based on the creation of a unified national telecommunications security posture under two principal heads, the National Carriage Boundary, and the NBN.