# Australian Government: Australia's 2020 Cyber Security Strategy

Submission by:

Shaugn S Vorster

PhD, MBA, BCOM, HDip(Met Eng), CGEIT, CRISC, GAICD

## 1 Executive Summary

Australia's Cyber Security Strategy should be seen in the context of Australian Territorial Security. This approach creates the opportunity to normalise initiatives with other Defence, Commercial and Societal security measures contained in relevant legislative instruments pertaining to the protection and securing of Australian Territory. This approach frames Cyber Security in terms that are National Security Based and of bi-partisan nature. The suggested strategic approaches are informed by this view and provide a framework for the definition of the Australian Cyber Security Strategy and a way forward to "weaponise" the response to threat vectors, as well as the leveraging of the commercial and societal opportunities that Cyber presents.

## 2 Cyber Territory

Australian Cyber Territory is a new concept. It consists of a virtual territory constituting all of Australian Cyber interests, interactions & transactions supported by human, physical & virtual infrastructure. "Ownership" of the Australian Cyber Territory would be a complex discussion given the fiercely held global independence & freedom that cyber space enjoys. Another way of viewing Australian Cyber Territory is that of an exclusive economic zone that requires protection.

## 3 Key Principles that should inform the Strategy

The reference below "Territorial Security, United States Institute of Peace" while dealing specifically with physical territorial security, provides a useful framework that may be extended to cyber territorial security.

Ref: Territorial Security, United States Institute of Peace, 12/09/2019; "https://www.usip.org/guiding-principles-stabilization-and-reconstruction-the-web-version/safe-and-secure-environment/terr" as adapted and framed in terms of cyber territory security.

- Cyber Security should be seen in the context of Australian territorial security i.e. as a subset of a range of security risk areas with appropriate risk mitigation.
- The Australian Cyber Security border points of contact are potentially infinite and span from within Australia's physical border, across its borders into Cyber Space. It is a State border akin to Australia's physical border. The Federal government should exercise control over the Cyber border in the same way that it exercises control over the physical border.

- The Australian Government seeks to provide broad perimeter security mitigations (physical and legislative controls) at the Cyber Border and has direct responsibility for State cyber assets, including connected critical infrastructure. The Australian Government may have an interest in

assuring that non-state cyber assets and related enterprises of significant national importance are protected.

- The owner/and or custodian of the data/cyber asset is ultimately responsible for managing and mitigating risk associated with that asset.

# 4 Necessary Condition: Australian Cyber Territorial Security

Cyber Territorial Security is a necessary condition in which ordinary Australian citizens can access and use cyber infrastructure, services and capability with relative freedom, within Australia and across its borders, including Cyber Space, wherever that may be. This implies that legitimate activities and freedoms (including freedom of speech and the right to privacy) are monitored and protected. Controlling Australia's Cyber Territorial Security is necessary to track what enters and exits the country or to prevent threats to security and legal commerce*. [ Author comment: This has implications for the unfettered movement of information, social media interaction and subsequent legal instruments noting the possibility of both internal and external destabilising elements e.g. election interference, the spread of radicalisation etc.]*.

# 5 Australian Cyber Territory Border

The Australian Cyber Security border points of contact are potentially infinite and span from within Australia's physical border, across its borders into Cyber Space. It is a State border akin to Australia's physical border. The challenge is maintaining the security, integrity and resilience of the access points, the transactional legality & continuity through the access point, as well as navigating the legal (commercial and political) complexities that arise where borders and territorial sovereignty are not clear cut.

Example One: Nation State X's cyber territory extends into Nation State Y's territory and vice versa. These points of intersection are grey. Should a dispute arise between citizen X and citizen Y, which nation states law applies and how does the state protect the interests of its citizens in the process? How does X manage the standards of goods and services from Y i.e. X may have stringent manufacturing/social standards for local production which Y may not have? Who has jurisdiction and is it enforceable?

Example Two: The physical territory access points to Australia are patrolled/ controlled/ managed by the Federal Government. Who does this for the Cyber Territory? Private companies under government contract? Companies with Australian allegiance? How does the government ensure that Australia always has continual and uninterrupted access to, and freedom of movement in, Australia's cyber territory?

# 6 Guidance on Cyber Territorial Security

## 6.1 Approach: Freedom of Information Movement

Freedom of Information Movement refers to the free flow of publicly available information and cyber services through cyber networks without fear of censorship or disruption, while threat actors, illicit commodities & services, and other sources of instability are restricted in movement. Enabling freedom of information movement has wide ranging benefits including promoting economic growth and social normalisation among communities. The role and rules around the use of Virtual Private Networks and their potential impact on Cyber Territorial Security may need to be assessed. In

practical terms, virtual private networks by their nature create “secret” access points through the cyber border, albeit for mostly legitimate reasons.

### 6.2 Facilitate consumption of information, goods and services

Establish legislative instruments on where to enable, limit or deny access to Australian Cyber Territory.

### 6.3 Deny movement to threats to Australian Cyber Territory

Establish legislative instruments and physical capability to limit, deny and or counter threats to Australian Cyber Territory.

### 6.4 Approach: Cyber Border Security

Cyber Border security involves managing the movement of information and services across Australia’s Cyber Border to ensure that these elements do not destabilise the country. Aspects of territorial security may include:

6.4.1 Physical Security: Ensuring that Australia’s inbound and outbound access to its Cyber territory is unfettered, resilient and secured. In addition, management and security of the points of contact between the Australian Cyber Border and other international and private cyber territories.

6.4.2 Information Security: Establishment of information sharing protocols and the monitoring of cyber border areas for crime and/ or information that may expose a crime/misfeasance, disinformation, movement of money, transnational organised crime, destabilising and anti-Australian threats from organisations, individuals and adversarial State Actors.

6.4.3 Customs and Export: Regulation and promotion of goods and services provided or obtained via the Australian Cyber Territory.

6.4.4 Actions taken to develop and maintain a world class cyber border security force for an indeterminate period.

### 6.5 Address Cyber Territorial Security in International Trade Agreements

If not already in place, address Cyber Territorial Security in terms of establishing a mutually beneficial means to protect and enhance Australia’s interests in the light of potential conflict or grey areas in legal precedence, disparate standards and jurisdiction.

### 6.6 Build Australian capacity for Cyber Territorial Security as a first order priority

While excellent work and progress has been made by the Federal Government and specific civil servants, unless there is a significant change in the way that Cyber Territorial Security is approached, it will remain under funded, under resourced and the threat and opportunity underestimated. Cyber Territorial Security should enjoy the same level of priority and care afforded to the protection of other Australian territories. The following questions may inform the motivation:

6.6.1 How long could Australia survive if its connections to Cyber space were impaired? What are the alternative connections if any? What arrangements are in place with our political partners to mitigate against total or partial loss of access i.e. Shared Satellite alternatives, Government owned alternative assets?

6.6.2 If the integrity of Australian Cyber Territory was in question, what would the political and socio-economic impacts on territorial security be? How would this impact our relationship with our trading and security partners e.g. Five Eyes Intelligence Sharing Network?

6.6.3 To what extent is Cyber Territorial Security currently under Australian control? What risks does this present and what are the mitigating actions? Is this good enough and sustainable given that the Australian Government must be prepared to perform Cyber Territorial Security operations for an indeterminate period.

6.6.4 What would be the economic, social and political benefits be if we viewed our cyber territory as the launch pad for a new economy?

# 7 Selected responses

The selected strategic approaches should be read in conjunction with the preceding discussion.

## 7.1 What is your view of the cyber threat environment? What threats should Government be focussing on?

7.1.1 The biggest threat to Australian Territorial Security is underestimating the importance and complexity of Australia's Cyber Territory. Under pinning this are two themes - complacency and resilience. This is further undermined by fear and a market driven response to cyber threats that can and does desensitise the Australian public into two modes – doing nothing because of a feeling of helplessness and/or being overwhelmed with mixed messaging; or a compliance driven tick box mode. This is compounded by the concepts and understanding of freedoms in the context of Australian Cyber Territory. The impetus and posture will change if a positive benefits approach is focussed on.

## 7.2 Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

7.2.1 www. Nationalsecurity.gov.au refers: State and Territory governments:

*7.2.1.1 maintain policies, legislation and plans within their jurisdictions*

*7.2.1.2 maintain counter-terrorism and consequence-management capabilities within their relevant agencies*

*7.2.1.3 have primary operational responsibility for responding to a terrorist situation in their jurisdiction*

*7.2.1.4 determine prevention strategies and operational responses to threats, including seeking assistance from other jurisdictions*

*7.2.1.5 actively consider the requirement for the declaration of a national terrorist situation*

*7.2.1.6 in a national terrorist situation, contribute to the national strategy.*

7.2.2 Protection of Australia's territorial security include threats that impact on Australia's economic and political stability, wellbeing and sovereignty. The definition of which actions taken by cyber threat actors fall into a Terrorism category, would need to be further clarified. This implies that mitigation and prevention of a cyber threat that is classified as terrorism / an act of aggression by a state actor, falls under the above remit.

7.2.3 Viewed through the lens of managing Cyber risk as an element of managing Australia's Territorial Security, it's clear that the Federal, State and Territory authorities, as well as Australian Citizens all have a role to play. This may require further definition and education.

7.2.4 It is also submitted that Australian Citizens have a duty and responsibility of care for their own wellbeing, and in their interactions with each other and the community at large. This holds true whether the interactions are of a private or commercial nature. There is a vast body of Australian law that underpins this. The question is however, whether Australian Cyber Territory specifically is adequately covered by these laws and protections. This is compounded by the definition and or agreement of what the limits of Australian Cyber Territory are, and the extent of its interfaces with other Country Cyber Territories are.

7.2.5 Following on the above comments and the generally accepted Information Security principle that "The owner/and or custodian of the data/cyber asset is ultimately responsible for managing and mitigating risk associated with that asset", Australian citizens (be it private or corporate) should actively participate in the securing of their own data, transactions & cyber interactions, and be held accountable as appropriate.

7.2.6 The key difference between Australian physical territory defence and cyber territory defence is the proximity and points of contact & inter action in the latter. This is analogous with seeing a documentary about war versus being a participant. All citizens engaging in and with Australian Cyber territory are in a potential war zone. There is no distance separation.

**7.3 Do you think the way these responsibilities are currently allocated is right? What changes should we consider?**

7.3.1 The threat to Australia's cyber territorial sovereignty should not be underestimated. It is a war that must be won. The responsibilities for management of cyber risk at Federal & State level need to be redefined. The scale and magnitude of interaction within Australia's cyber territory dictates a more nuanced approach than referred to in www. Nationalsecurity.gov.au. The premise that Australian Cyber Territory is a valid construct, will substantially change the approach, methodology, responsibility & resourcing of the Australian Cyber Strategy.

**7.4 What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?**

7.4.1 Resilience – The question is, is how much of Australia's cyber territory lies in the hands of Australian private institutions, or other non-Australian institutions with limited loyalty to the Australian State? What actions should Government take to protect and maintain unfettered access? What partnerships should we have with other nation states to protect/ promote this view? Can it even be possible that the defence of Australian Territory be subcontracted to a third party?

7.4.2 Advocacy - Change the messaging and educate, both at corporate and citizen level. This is the single most important step in securing societal change and awareness. Bear in mind that average citizens are closer to the points of interaction in the cyber territory and hence more exposed. This approach creates a wider cyber threat response capability

7.4.3 Legislate - Annual reporting of actions taken to improve and leverage the benefits of cyber security initiatives. Broad social security awareness promotes protective, integrative behaviour & strengthens the broader territory security perimeter i.e. resources.

**7.5 How can Government maintain trust from the Australian community when using its cyber security capabilities?**

7.5.1 There should be no differentiation between protections that apply to Australian Cyber Territory versus that of any other Australian Territory.

**7.6 What customer protections should apply to the security of cyber goods and services?**

7.6.1 See preceding comments

**7.7 Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?**

7.7.1 The answer to this question is informed by whether the Australian Cyber Territory exists or not.

**7.8 Is the regulatory environment for cyber security appropriate? Why or why not?**

7.8.1 Possibly not. See preceding comments.

**7.9 What specific market incentives or regulatory changes should Government consider?**

7.9.1 Significant alignment of law and regulation in line with other Australian physical territory. Extension of law and regulation to deal with issues unique to the Australian Cyber Territory.

**7.10 How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?**

7.10.1 The acknowledgment of the fact that Australian Cyber Territory is a true, and requires an appropriate Federal, State and Territorial response will drive standards and grow an appropriate resource response: a typical case of supply and demand matched to skill level and standards required.

**7.11 Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?**

7.11.1 The premise that there needs to be growth of the Cyber Insurance market or indeed that there needs to be a Cyber Insurance market at all is flawed and debatable.

**7.12 How can high-volume, low-sophistication malicious activity targeting Australia be reduced?**

7.12.1 The role of ISP's in providing territorial threat response and mitigation needs to be pursued. The technology exists today to identify malicious activity of this nature.

**7.13 What changes can Government make to create a hostile environment for malicious cyber actors?**

7.13.1 Shut them down and pursue a response from the originating countries in terms of reciprocal trade agreements e.g. trade agreements may stipulate that cybercrime activities originating from within the borders of signatories to that agreement will be dealt with in an agreed way and to a particular standard of international law. Failing this, reciprocal penalties would apply, or something of a similar punitive nature.

# 8 Acknowledgement