The Hon Peter Dutton MP
Minister for Home Affairs
Parliament House,
Canberra ACT

October 31, 2019

Dear Minister,

Second Submission to Australia's 2020 Cyber Security Strategy Call for Views

Thank you for the opportunity to contribute to the development of the nation's next Cyber Security Strategy.

I have already responded with a submission dated October 30 for public viewing focusing on taking a public health approach to the cybersecurity problem.

In this second submission, I would like to focus on national strategy and national security priorities.

I write this from over 30 years of international and Australian public sector, international policy, and commercial cyber security experience. In particular, I have been close to national security discussions and actions in Europe, North America, and the Middle East over the last twenty years – as well engaging in dialogue with Australian agencies. I also have worked closely with the international Internet technical community to ensure a single globally interoperable Internet – but at the same time promoting security operations and rules for network operators and users.

The overarching goals of the nation's Cyber Security Strategy should be:

1. Defend the country
2. Keep the democracy stable
3. Protect the economy

The rise of the networked world presents Australia with a profound change in epoch. I do not write this flippantly. Not only do the rapidly changing and expanding capacities of the Digital Socio-Economy present unprecedented changes, opportunities and challenges for nearly every aspect of Australian life (e.g. the future of work, skills, trade patterns, income distribution, social perceptions, entertainment, aging and health care, etc.) but they also upend in grand and also nuanced ways the paradigm of Australian national security that has been in place for at least a century.

1. Defend the country

The Australian strategic equation has completely changed. The challenge for the Australian government is both comprehensively to adapt to this and to engage the population in understanding its implications. As a nation we all need to own this.

The general population has a mis-founded yet deep confidence in geographic isolation:

- For thousands of years, geographic isolation has been the dominating input for the security equation for Australian populations. Only in 1788 and 1942 has this overarching feature failed or nearly so.
- Australian defence posture and capital expenditure since at least the Dibb Report has been, inter alia, directed to a strategy of controlling the air-sea gap to the north of Australia and deterring an invasion of the Australian mainland. If pushed, most of the Australian population would identify ships, submarines, aircraft and the troops as the embodiment of this "keep our isolation" strategy.
- While intercontinental ballistic missiles have partly eroded the benefits of isolation, since the end of the Cold War their risk to Australian territory has diminished significantly.
- However, a global, deeply-interconnected information economy has completely changed this defence-in-depth equation. It has also dramatically "privatized" the battle space as over 90% of IT systems and networks are run by the private sector.
- Almost all Australians and Australian economic actors are connected continuously to a global network on which thousands of hostile forces are daily seeking to gain financial, intellectual property, political and military advantage against Australian interests.

Isolation is dead. But most Australians and Australian institutions do not really understand this. The challenge for the Australian government is engage the Australian population in a dialogue that puts cybersecurity not just in economic and personal safety terms but also in more pressing national defence terms.

I would recommend that this new national perspective requires three actions:

a) Change the capacity and mindset of the private sector (and universities and local government)
b) Actively develop and expand an international network of support beyond the usual five eyes intergovernmental arrangements to build capabilities available to Australia and to actively test the focus and efficiency of Australian government spending on cyber security and related capabilities (for instance, Artificial Intelligence).
c) Establish the institutions and flexibility to support the development of a sizable cyber security workforce reserve for crisis response.

A. Change the capacity and mindset of the private sector

The reality of daily active cyber operations by big and medium sized powers, and the rising regional and international geopolitical tensions, means that the Australian government should plan with a mindset that major Australia military and espionage operations with significant cyber offense and defence aspects, are only a matter of when, not if. Further, such operations will be played out over Australian and international private sector networks and IT capabilitlies. The leaders of the Australian business community, especially in the sectors of critical infrastructure, and state

governments should be engaged in an ongoing planning and exercising discussion to that end. An appreciation of the risk and the need for the private sector to respond (an attitude not dissimilar to that of Essington Lewis, the general manager of BHP in the 1930s) should be more broadly engendered across Australian boardrooms.

I am aware that much effort has been made by Commonwealth agencies to improve the cybersecurity engagement with the private sector both before and since the 2016 Cyber Security Strategy. The establishment and activities of the Joint Cyber Security Centre have been important. This is to be applauded. But I would also warn about what may look like effective outreach from a Canberra perspective often does not look so effective from the perspective of the commercial cities. I can share that from my conversations over the last 2-3 years with many board directors, company executives, state and local government executives and university deans in Brisbane, Sydney and Melbourne: few see cybersecurity beyond a cyber-crime perspective and a surprising number don't think there is a big threat to their company. While a number see cybersecurity as national security issue in terms of espionage, only a mere handful see cybersecurity as a national defence issue. Few are aware of the Joint Cyber Security Centres – and some CISOs have reported to me that their interactions with the JCSCs has been limited. I recognize that this is a subjective statement. But I share it as a tonic to the "we have an agency and a program for that therefore it is covered" mindset that sometimes can be prevalent in government.

I would recommend that the government seek to counter the above concerns by achieving two outcomes:

- A measurable increase in the understanding and engagement of boards and C-suites of Australian companies that cybersecurity is both a national defence issue as well as a risk issue for their business
- A promotion and measure of increased resources by Australian companies to cybersecurity, including resources which could be ultilised for national defence in a period of crisis.

Some steps which I would recommend should be undertaken to achieve these outcomes include:

I. A continual national engagement program which ensures that meetings of the key industry associations and the boards of the top 300 publicly listed company and identified major privately held companies receives annually a tailored address/meeting with a Minister or senior official on risks to the country as well as to their industry. (During the more innocent and optimistic turn of the century the Ministers and Senior Executives of the National Office for Information Economy conducted over 200 such speeches and presentations annually extolling the benefits and needs for the adoption of the new network technologies.)

    a. During these engagement meetings, Commonwealth representatives should urge recruiting and training resources to be dedicated by the companies to mitigate their own risks – but also to make available skilled resources to the sector or the nation at a time of crisis.

II. Follow the lead of New York state and require medium and larger companies to:
    a. appoint a Chief Information Security Officer (the individual could be an employee or outside contractor);
    b. establish a cyber security policy annually approved by the Board.

My experience of dealing with New York based firms over the last decade is that the introduction in 2017 of the New York State Department of Financial Services' cybersecurity regulation had a big impact in deepening the attention to cyber security administration within firms. Now addressing such details is just part of regular business practice.

New York exempts companies having less than 10 employees (including any independent contractor) or those companies with less than US$5,000,000 in gross annual revenue (or less than US $10,000,000 in year-end total assets). I note that Australian tax law applies a small business concession to entities which have aggregated annual turnover less than $10 million.

More detailed aspects of the New York rules could be required only of Australian publicly listed companies and private companies with turnover of more than $50 million. Their cybersecurity policy could address the following areas to the extent applicable to the organization:

a. information security;
b. data governance and classification;
c. asset inventory and device management;
d. access controls and identity management;
e. business continuity and disaster recovery planning and resources;
f. systems operations and availability concerns;
g. systems and network security;
h. systems and network monitoring;
i. systems and application development and quality assurance;
j. physical security and environmental controls;
k. customer data privacy;
l. vendor and Third Party Service Provider management;
m. risk assessment;
n. regular cyber security awareness training; and
o. a written incident-response plan.
p. Such companies would also be required to monitor and test their program.

III. Measure the amount and trend of cyber security training spend by companies and public entities.

IV. Continue national/international exercises like Cyber Storm II and sector specific exercises. But ensure that these exercises include periods of disruption to the electricity supply (my experience in the US is that critical infrastructure sectors do not often exercise "out of sector" risks. Indeed at least some US financial services critical infrastructure has built contingency plans about cross-storing critical data which does not necessarily consider the impact of all relevant data facilities being within the same electricity grid.)

V. Conduct further national exercises on politico-military scenarios which involve both the ADF and critical infrastructure. Bringing the attention of private sector leadership to preparedness for scenarios of information warfare and preparation of the eyber battlefield is an essential part of educating Australian corporate leadership that cybersecurity is a public/private national defence issue.

B. Develop and expand an international network of support

As I have argued above, the Australian government should plan with a mindset that major Australia operations in the region with significant cyber offense and defence aspects, are only a matter of when, not if. With such a mindset, the Australian Cyber Security Strategy should adopt some of the strategies of countries operating under threat. In particular, it should seek to maximise the size and expertise of the cyber forces available to the Australian taxpayer. Some steps to achieve this should be:

I. Follow the lead of the Israelis, French, South Koreans and Germans in the US, formally or informally recruit a network of Australian expats in the North America and Europe who are locally involved in cybersecurity and who can mobilise local expertise to harvest both policy advice and technical advice/capability. For instance, the French American Foundation runs regular meetings of its cyber security initiative bringing together high level military/government and business leaders from both countries to discuss cyber issues: https://frenchamerican.org/initiatives/cyber-security/. This group also conducts governmental and commercial discussions on the fringes of the meetings. The Israelis take the approach down to the city level. Israeli cyber security companies and venture capital firms joined a New York City government project: the new Cyber NYC initiative: https://edc.nyc/program/cyber-nyc The South Koreans look for similar expertise linkages utilizing a link between KOTRA and industry leaders and incubators.

   An Australian equivalent initiative should be directed to identifying Australian expat experts as well as leading US and European cyber (governmental and non-governmental) expertise and creating long term relationships and expertise sharing. In the US, it is important to not just focus on Silicon Valley – the US east coast has much of the cyber expertise. Including Australian cybersecurity companies should be part of the strategy, but the goal is not just to aid Austrade's existing export assistance mandate. The focus should be on developing long term relationships and ensuring the easy transfer of world leading expertise and technical capability to Australia.

   One of the benefits of such an expat group would be to leverage the broad based goodwill towards Australia (significantly a product of being allies in the wars since 2001) among US government, companies and especially cyber experience veterans to:

   a. Augment existing Australian capabilities and capacity: attracting skilled US personnel to Australia is something which could be easily promoted, especially with such initiatives as the recently announced Global Talent - Independent Program.
   b. Test Australian plans and spending priorities: the scale of the US market is such that many of the leading technical research and deployments are taking place or are visible to major players. When the Australian government is considering funding projects to directed to innovation in the areas of cybersecurity, artificial intelligence, Internet of Things etc, a useful test of priorities and efficiency would be to run the programs past major US users of technology. For instance the CIOs/CISOs of the big 6 banks in the US would be an insightful group against which to test whether an area is indeed groundbreaking or whether it is now more populated with companies and solutions.

II. Encourage and support the Australian technical community to establish broad and lasting links with their colleagues, especially in similarly minded democracies.

Since the 2007 Russian cyber-attacks on Estonia I have met with several groups which have claimed victory in responding to these attacks – Toomas Hedrick Ives, other Estonian government officials, NATO people, etc. But the role of one group is mostly not known by the government actors to whom I have spoken. The attack coincided with a RIPE NCC (the Regional Internet Registry for Europe) meeting in Amsterdam and many of the civilian network operators and engineers attending the meeting peeled off to help their Estonian network operator colleagues – particularly redirecting traffic across Europe and countering Distributed Denial of Service Attacks.

This is only one example of the technical community working to help each other during particular attacks.

There are several lessons which can be learned from these instances:

a. Maintaining a wide range of personal connections in the international technical community really matters
b. Civilian network/IT/software engineers can be a very valuable resource at a time of crisis, especially if they are willing to act on personal allegiances and trust and not be constrained by concerns about lability
c. An international group of operators geographically distant to the networks being attacked can be very effective – and can be an important force multiplier for a small or medium country.

The Government should promote Australian attendance at such technical meetings as the IETF, IEE, APNIC, ARIN, RIPE NCC, Apricot, Nanog, ICANN. The importance of technical staff attending should be made clear to company senior executives. Australian attendance at such meetings should be measured and tracked. Although attendance costs for companies may be tax deductible, perhaps such costs could also be subsidized through inclusion in existing business programs such EMDG or R&D development grants.

C. Develop of a cyber security workforce reserve for crisis response.

As noted above, it has been my experience that Internet technical people can be very responsive to peers in trouble where the relationships and trust networks are in place to support swift mobilisation. I would recommend that the Australian government(s) take three steps to assist the speed and scale of such mobilization:

I. To support swift informal responses change liability rules to enable civilian (and government) cybersecurity resources can be quickly mobilized on a volunteer basis to different companies/government under attack by adversaries (particularly nation state adversaries). Volunteer technical people should be granted at least the same level of civil liability protections as provided by the various State Emergency Service Acts.
II. To support a greater scale of formal mobilization:
    a. Establish a civilian reserve (like State Emergency Service) type service for cybersecurity resources be available to mobilized to respond to major civilian type attacks.

b. Establish dedicated ADF cyber security reserve units – in particular, look to spin up dedicated cyber units as part of the University Regiments– potentially not requiring the same physical fitness requirements.

2. Keep the Democracy Stable

The increased use of Internet platforms as a cheap and large scale vector for information warfare is one of the most troubling aspects of the present cybersecurity environment. The activities of such bodies as the Russian Internet Research Agency has shown that democracies like Australia face a new and systemically challenging threat to our governance and social cohesion.

Some of the best responses to the increased threat of information warfare against Australia is for the Australian political leadership to seek to ensure that political debate continues to be largely informed by the traditional economic inputs and issues. Further general support for institutions like the parliament (including question time) , the public broadcasters, compulsory voting, key economic and social analysts in the community and the media should be encouraged – and foreign attempts to target this support strongly countered.

Some specific efforts the Australian government(s) could take to defend our democracy are:

I. Educate the public at large about the tactics and motives of information warfare,

II. Educate students about the need to evaluate online communications in the possible information warfare. There is not a need for a new subject, but rather I would suggest making amendments/additions to parts of the existing curriculum. In doing this, Australia could learn from the Finnish example of having entered details across the curriculum to educate children then adults about the fake news/information warfare practices of their neighbours. Australia could build on the safety online framework in schools.

III. Support the ACCC's recommendations in Chapter Six of its Digital Platforms Report in June 2019 for an independent regulator to:
   a. monitor, evaluate and report on the actions digital platforms are taking to improve and support credibility signaling; and
   b. oversee digital platforms' actions to address disinformation and malinformation

IV. Get closer to the Europeans on policy and to the US on capabilities. For instance, follow the lead of the October 2019 decision of the European Court of Justice on Facebook which founded that
   a. If an EU country finds a post illegal in its courts, it can order websites and apps to take down identical copies of the post
   b. Platforms can be ordered to take down "equivalent" versions of an illegal post, if the message conveyed is "essentially unchanged"
   c. Platforms can be ordered to take down illegal posts worldwide, if there is a relevant international law or treaty

   Adopting such a set of rules would be very helpful in reinforcing the ACCC recommendations on digital platforms and disinformation. An Australian

adoption of such a rule would include all platforms, including the Chinese platforms which are an increasingly influential mechanism for social and political intercourse among parts of the Australian community – and which are subject to Chinese government censorship.

V. Finally, review carefully the recent penchant in Australian government for combining roles and resources into single entities in the name of efficiency. It has been the experience of the Internet Community that single mechanisms often become honey pots for attack and single points of failure or poor design. One of the reasons for the resilience to attack of the Internet's Root Server System is its diversity – of ownership models, operating systems, software, mirroring and network. Aggregating data resources may be initially attractive for efficiency reasons but often results in diminishing resilience and increasing the attractiveness for targeting. And such targeting can be an easy method for an adversary to undermine public confidence in the Australian system of government.

3. Protect the economy

My submission of 30 October made several recommendations about addressing market failures which will help to protect the Australian economy. It is submitted that undertaking the recommendations in the section "Change the capacity and mindset of the private sector" above will also contribute to protecting the Australian economy.

To conclude, it is essential that Australia's 2020 Cyber Security Strategy maintain a focus on the national defence at a time when the reality of major Australia operations with significant cyber aspects conducted over privately held networks and facilities is only a matter of when, not if.

Yours sincerely,

[redacted]

Dr Paul Twomey
CEO

Argo P@cific Pty Ltd
ABN: 16 091 389 356
GPO Box 3468
SYDNEY NSW 2001
Ph: +61 2 8236 7999
Fax: +61 2 8236 7913