COMMUNICATIONS
ALLIANCE LTD

Cyber and Critical Technology International Engagement Strategy (CCTIES)

Communications Alliance submission
to the
Department of Foreign Affairs and Trade

16 June 2020

TABLE OF CONTENTS

COMMUNICATIONS ALLIANCE

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

1 INTRODUCTION

Communications Alliance welcomes the opportunity to provide this submission in response to the Department of Foreign Affairs and Trade (Department) call for submissions on the development of Australia's Cyber and Critical Technology International Engagement Strategy (CCTIES).

The Department requested that submissions consider at least one of the following questions:

1. What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?
2. How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?
3. What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?
4. How should Australia pursue our cyber and critical technology interests internationally?
5. How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?
6. What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

In the following, we will touch on several of these questions but with a somewhat greater focus on Questions 1, 4 and 5.

2 CONSIDERATIONS FOR A CYBER AND CRITICAL TECHNOLOGY INTERNATIONAL ENGAGEMENT STRATEGY

2.1 General Remarks

It is hard to overestimate the importance of a well-executed international cyber and critical technology (in the following, we will use 'cyber+' as a shorthand) engagement strategy: many aspects of modern life are already digitised and 'cyber', and we can reasonably expect that pretty much *all* areas of our lives will be part of the cyber space in the next 10 years. Naturally, as owners and operators of the underlying infrastructures, the communications and IT industries have a strong interest in the development of an effective and coherent international cyber+ engagement strategy.

However, we note that the digitisation of all aspects of the modern state mean that all industries and sectors as well as citizens ought to be part of this important discussion. Therefore, we commend the Department for its decision to re-calibrate the 2017 efforts on the creation of an international cyber engagement strategy to now also extend to critical technologies which includes, so we assume, artificial intelligence (AI), big data analysis, virtual reality (VR), 5G and quantum technology, just to mention a few.

A cyber+ engagement strategy is (or ought to be) almost inevitably international in nature given the cross-border nature of data and increasing globalisation. It is the cross-border nature of computer systems, the ease of data transfer globally and the global nature of supply chains that necessarily make any viable strategy an international affair, especially for open economies that rely on international trade and relationships for the running of their economies and their national security.

Therefore, it appears that individual elements of an engagement strategy, including those pertaining to cyber security, such as the Telecommunications Security Sector Reform (TSSR), data retention legislation, legislation in relation to international data exchange for law enforcement purposes as well as copyright and website blocking legislation etc., ought to flow out of an international strategy that takes into account and attempts to align with the approaches taken by Australia's key trading partners, where feasible.

It should be noted that a cyber+ engagement strategy is not equivalent to a cyber security strategy. While cyber security is a key, if not *the* key, element of a cyber+ engagement strategy, the latter goes beyond the "protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide"[1] and encompasses the best possible use and the stimulation of continuous innovation in the use of such systems, with the aim of maximising economic and social benefit.

Given the very dynamic nature of the cyber space, any strategy in this field must be flexible enough to adapt to technological and societal change. Consequently, an ongoing dialogue between all stakeholders, including the general public and civil society organisations, will be imperative for the effectiveness of a such a strategy.

We consider that there are three specific outcomes that an international cyber+ strategy should seek to deliver:

- Increased cyber literacy and security, nationally and in our key trading partner countries;
- Harmonisation of relevant legislation, the development/adoption of open technology standards and a coherent (and timely) approach to the proliferation of new key technologies; and
- Improved international coordination and development of effective enforcement mechanisms at an international level.

However, we also note that current national approaches to cyber security and other cyber-related matters would benefit from streamlining to allow for the most effective and efficient pursuit of an international cyber+ strategy.

2.2 Streamlined International Engagement

As noted in previous submissions, Australia's cyber landscape is complex and involves a multitude of stakeholders and Government departments and agencies. Similarly, a considerable number of international organisations focus on cyber-related matters.

We identified a several regional and global fora that engage with cyber security and that, we believe, are relevant to Australia's strategic interests. However, it is not always clear to us whether Australia engages in all of those fora, and if so, through which organisation/means of representation it participates, whether this engagement is effective and whether additional or different efforts would be required, particularly also in areas that do not specifically relate to security.

Global fora:

- Organisation for Economic Co-operation and Development's (OECD) Working Party on Security and Privacy in the Digital Economy
- Internet Governance Forum
- United Nations (UN) Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
- International Telecommunication Union
- Global Forum on Cyber Expertise
- Global Conference on Cyberspace

[1] https://en.wikipedia.org/wiki/Computer_security

- Commonwealth Telecommunications Organisation

Regional Fora

- Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group
- Association of Southeast Asian Nations (ASEAN) Cyber security Cooperation Strategy
- East Asia Summit

We would also like to see a comprehensive and structured consultation process to assist preparing positions that are put forward at regional or global fora. We are not aware of such a structured approach but note that industry does receive occasional ad-hoc requests for input.

As part of the development of an international cyber+ engagement strategy, it will be important to gain a better understanding of whether the involved departments/agencies engage with overseas counterparts and, if so, with which organisations/agencies and on what specific issues. The resultant picture ought to be shared across relevant stakeholders.

In a second step, it could be useful to establish a central coordination point within the Department to enable industry to access those overseas Government stakeholders in an effective and coordinated manner, where required. Such a central outreach point within the Department would also provide industry with an effective feedback point when Government departments/agencies seek to put forward an Australian position on specific cyber-related matters.

Key trading partner nations could be encouraged to mirror similar access point arrangements (if not already existent) for their national industries.

We note that, overall, a streamlining of national organisations, functions and processes could be useful. However, this is not to say that all cyber-related functions ought to come under a 'single roof' as it will be important to retain appropriate checks and balances. It will also be important to continue to drive international cyber+ engagement from a cross-sectoral base and a background of consolidated international expertise across an array of international projects and relationships. Where appropriate, we encourage the Department to leverage off already existing technical expertise within the Australian Signals Directorate (ASD)/Australian Cyber Security Centre (ACSC).

It is important to ask which other areas of responsibility in the field of cyber engagement (other than cyber security) Government, industry, academia and other stakeholders ought to address to fully harness the advantages of the cyber space to Australia's (and global) advantage. For example, the international harmonisation of data and privacy laws, the development/adoption of open technology standards, the identification of a toolbox of appropriate and effective risk management measures and a coherent (and timely) approach to the proliferation of the internet of things (IoT), artificial intelligence (AI), cloud platforms, 5G and fibre networks immediately come to mind in this context.

Australian businesses, as most other nations, make use of commercial advantages outside Australia and outsource some of the strategic and/or operational functions to other countries, e.g. European Union, India, Philippines, US, UK, Singapore and Japan. China plays an important role independent of any potential outsourcing arrangements due to the large quantity of devices that originate from there and the potential to greatly impact any nation's cyber space. An analysis of businesses' data sharing arrangements as set out in privacy policies may reveal further countries of interest in this context.

In this context we note that the December 2019 Discussion Paper *Australia's 2020 Cyber Security Strategy* did not place the proposed strategy sufficiently into such an international context. Further consideration ought to be given how the strategic approach envisaged for Australia relates to efforts in other nations, especially Australia's key trading partners and global industry standardisation organisations (e.g. 3GPP) and alliances (e.g. GSMA), and

how it would contribute to the unification of global standards, harmonisation of relevant legislation, appropriate and effective risk management measures and international cooperation.

2.3 Cyber Specialist Resources

One of the biggest challenges posed by the cyber world is the attendant security considerations. For many organisations, and Australia in general, there is a constant need for expert resources to cope with the evolving scope of cyber security threats. This demand for cyber security specialists is not met with an equal supply available to all Australian businesses. We would suggest that this may also be the case in many other nations. The shortage of supply may be partly a result of lacking tertiary (and other) education opportunities in this field and is likely to be exacerbated by fierce competition for qualified resources from other well-resourced sectors, such as the financial services and insurance sectors. As matters stand today, communications industry members have highlighted a shortage of supply of specialist resources in various areas, e.g. in forensics, penetration testing, incident management and risk assessment.

In addition, it would be prudent to broaden the scope of any strategy to address skill shortages to also include the production of experts in policy, psychology, law etc. which are all areas that will play an important role in long term strategies to enhance cyber security.

Against this background, industry urges Government to develop a cyber strategy(nationally and internationally) that includes a targeted program to develop and retain Australia's expertise in this area to ensure that local resources are available to all industries and all players within those industries.

It could also be useful to investigate international models for developing cyber (security) capacity, their effectiveness and, where feasible, applicability in an Australian context. An international cyber+ strategy ought to give consideration as to how it can build effective and enduring relationships with international educational institutions and how overseas-trained resources could be brought to and retained in Australia. This may involve removing legal barriers (e.g. visa conditions). It may also be useful to explore cross-national (or even global) qualifications that target specific cyber-related needs to allow for the free movement of experts in a global cyber space.

Given the fast pace of evolution in the cyber security arena combined with the level of technical expertise required for practical industry application, educational institutions/academia and industry from all sectors must cooperate very closely to ensure that education remains relevant and meets demand as technology evolves. Consequently, any education program ought to include mentoring initiatives, graduate programs (including substantial work experience), and grant schemes aimed at fostering innovation and creativity in this space. In an international context, this could also include providing incentives for global organisations operating in Australia to develop or deepen intra-organisational exchange programs, career opportunities etc.

2.4 National and International Standards and Cooperation

We have argued in previous submissions, that national cyber literacy, especially in the field of cyber security, of individuals and businesses ought to be improved through a consistent approach, consolidated messaging and potentially Government-led nation-wide campaign. However, it is key to understand that Australia will benefit if not only its own networks and critical infrastructure are secure (to the extent possible) from external attack but also through improved security of foreign networks which make it harder to serve as a base for launching cyber attacks or as the staging post for phishing or other forms of fraud and deception online.

Therefore, industry supports global efforts towards a standardised security development and solution design, referred to as Security Assurance Methodology (SECAM).[2] There is a real risk that uncoordinated global efforts in this area will lead to a diverging set of security requirements, which would jeopardise not only interoperability, but make security that much more complex to guarantee. Global standards and best practices are therefore fundamental to the efficient handling of threats – especially given that a large share originate across national borders – as well as to building economies of scale, avoiding fragmentation and ensuring interoperability. Therefore, it is essential that stakeholders, including operators, vendors, regulators, policymakers and IT-focused companies as well as players from other industries, work together to set common and open security standards that specify what needs to be secure and protected, rather than mandate the use of a particular technology, i.e. industry supports an independent process compliance/validation scheme rather than fragmented, national certification schemes for devices and IT systems, or expensive, time consuming certifications like, for example, the Defence Level Common Criteria (CC).

Beyond standards, collaboration among relevant stakeholders can encompass a number of practical areas, including information exchange, threat analysis, performance analysis, sharing of best practices and encouraging cutting-edge research. Given the proliferation of the IoT, cooperation with other connected infrastructures (at a global level) such as energy, transport, health care, resources, automated manufacturing, agriculture etc. will be of paramount importance.

2.5 End-User Trust and Security

It will be difficult or even impossible to address the issue of end-user trust in Australia's cyber space without also dealing with the question of how to balance civil liberties with the (actual or perceived) need by Government and industry to interfere with those civil liberties to safeguard against cyber (or other) harms.

Similarly, it will be key that national and international policy frameworks successfully balance the needs for robust security measures, including end-to-end encryption, with requirements for the purpose of law enforcement and the prevention of serious crime.

Against this background, it will be critical for Governments to resist the temptation to seek far-reaching and/or very broadly defined powers to control critical infrastructure without rigorous and independent checks and balances and appropriate transparency.

Although others are better placed to lead the debate on this matter, we do highlight that the recent tendency to rush legislation through Parliament without proper consultation with industry and other stakeholders and in disregard of expert advice, is detrimental to an informed debate on the consequences of such legislation on this delicate balancing act. As the (unprecedented) international reaction to the passage of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* has highlighted, while Australia's legislative processes remain the prerogative of our internal political processes, the consequences of our cyber-related legislation can have far wider consequences and should, accordingly, be considered with a view to its global consequences.

It is also important to raise the question of whether consumers are sufficiently informed about the cyber security of goods and services that they purchase – and which are usually imported from overseas – and whether those goods and services are actually secure. This question is even more pertinent in the context of the IoT and the expectation that in 2022 the average household will have 37 connected devices, ranging from smartphones to connected cat flaps, televisions, digital assistants, baby monitors, security cameras and

[2] Security Assurance Methodology (SECAM) establishes security requirements not just for products but also for product development processes. According to proposed SECAM rules, accreditors will verify a 3GPP manufacturer's overall capability to produce products that meet a given set of security requirements, which will eliminate the need for explicit certification on a per product basis, while also encouraging a solution based view.

refrigerators. The fact that, in the near future, everything will be connected makes a 'secure by design' approach imperative.

While security for traditional mobile devices such as mobile phones, tablets etc. would benefit from further improvements, overall security of such devices and the concept of security by design for those devices is reasonably well-established. However, as security scares around hacked baby monitors and smart TVs demonstrate, security for many devices connected to the internet leaves a lot to be desired.

One way of driving this outcome would be for industry to develop a trust mark for connected consumer devices which, similar to the water efficiency rating of washing machines or the health star rating on packaged food, provides consumers with a simple and clear indication of the security of the connected device that they are intending to use. If consumers are adequately educated about the benefits of secure products (and the significant risks of those that are less secure), they will demand and buy secure products, thereby driving a greater focus on secure design on the part of developers and manufacturers. Over time, it is conceivable that shopping outlets will seek to differentiate themselves from competitors by only selling devices with a certain cyber security star rating, similar to supermarkets advertising that the food they are selling does not contain any artificial colouring.

In the absence of a global trust mark and/or global underlying standards, such a trust mark could be created through a (self-)accreditation and/or testing program on a national basis.

Significant initial work has been undertaken by our members and members of the IoT Alliance Australia (IoTAA), also a not-for-profit organisation, to develop such a trust mark. It would be timely and appropriate for Government to provide funding to further this worthy initiative.

Notwithstanding the above, it should be clear that the development of the criteria and security standards that form the basis of any trust marks must be developed in an international arena, with subsequent rigorous enforcement by the responsible national agencies. The development and use of the CE mark (to indicate conformity with health, safety, and environmental protection standards for products sold within the European Economic Area) serves as only one example that cross-national trust or certification marks are indeed a realistic possibility. Therefore, any international cyber+ strategy ought to analyse any existing structures currently enabling Australia's participation in such developments and, where necessary, seek to improve on those structures.

2.6 Inter-Jurisdictional Frameworks

As all parties involved are likely to attest, inter-jurisdictional investigations of cyber issues can be exceedingly difficult due to lack of sovereignty, lack of resources, diverging or even conflicting priorities or all of the above. Depending on the matter at hand, even national investigations or initiatives can be cumbersome due to different legal requirements and/or Governmental roles and responsibilities.

Companies operating across borders or wanting to outsource parts of their operations or data storage equally feel the burden of having to comply with different legal requirements.

The creation of inter-jurisdictional frameworks will be key to the maximisation of the economic and social benefits and the minimisation of security risks that the cyber space brings with it. Unfortunately, one can also assume that this task will also be one of the most difficult to achieve. Nevertheless, considerable efforts by Government, private sectors and academia ought to be made to progress internationally applicable and enforceable frameworks as quickly as possible.

The cross-border nature of data, its increasing commercial value – in large parts due to vastly improved analytical capabilities (big data analysis) – and the soon complete digitisation of our civil societies, defence systems and Government apparatus, mean that ownership, sharing and protection of data across borders and jurisdictions will be vital for the maximisation of economic benefit and the smooth operation of societies, including the

prevention of crime and the enforcement of law. With significant parts of the world's population are still without regular or no access to the internet, a well-designed international cyber engagement strategy would provide a useful blueprint for developing nations without such strategies once they reach a critical point of digitisation. Those developing nations themselves, but also (maybe even more so) highly digitised nations around the globe stand much to gain from a secure and coordinated growth of the cyber space of the developing world.

It is, therefore, imperative that we engage on an international level to drive the development of international data frameworks. For example, it has been suggested to tie the protection of data to the location of users, i.e. to create a 'virtual sovereignty', by binding the laws of each country to the location of the user who created the data at the time the data was created.[3] While this would require international treaties and is not without challenges, e.g. when companies would be forced to abide by laws of states that they do not consider democratic etc., it appears that an international approach to data ownership, sharing and protection is unavoidable. While we do not intend to advocate for a specific approach of how to address this complex issue, the above example may be illustrative of the kind of inter-jurisdictional efforts that are required.

The key issue – and difficulty – to be considered when designing data and privacy frameworks will be how to maximise the economic benefit from data by allowing the private sector and academia to exploit its economic value or to use it for research that directly or indirectly will generate benefits for society while simultaneously allowing Government to protect its citizens.

However, independent of the aforementioned difficulties of creating inter-jurisdictional frameworks, we believe that ultimately a key objective of the international cyber+ engagement strategy must be the pursuit of effective (yet balanced) enforcement mechanisms (of inter-jurisdictional frameworks) at an international level that will result in collective action against the source of cyber threats and will facilitate the development of the cyber space to maximum social and economic benefit.

3 CONCLUSION

Communications Alliance and its members look forward to continued engagement with the Department of Foreign Affairs and Trade and other departments and agencies on the development of an effective and efficient Cyber and Critical Technology International Engagement Strategy.

As outlined in this submission, we believe that a cyber-literate nation will be key to a successful national and international cyber+ strategy. National structures ought to be analysed, and where required enhanced, to ensure an effective engagement with overseas Government agencies, fora and organisations to allow Australia to optimally participate in global cooperation efforts and the development of standards.

It is imperative that Government, in close consultation with the private sector, drives the development of inter-jurisdictional security and data frameworks and actively participates in (and funds) the work required to ensure that the IoT can be fully exploited to Australia's advantage.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

[3] Andrew Burt, "Virtual sovereignty can help govern our data", 6 February 2017, Financial Times

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507