COMMUNICATIONS
ALLIANCE LTD

International Cyber Engagement Strategy

Communications Alliance submission to the Department of Foreign Affairs and Trade

31 March 2017

TABLE OF CONTENTS

INTRODUCTION

Communications Alliance welcomes the opportunity to provide this submission in response to the Department of Foreign Affairs and Trade call for submissions on the development of Australia's inaugural international cyber engagement strategy.

About 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.

CONSIDERATIONS FOR AN INTERNATIONAL CYBER ENGAGEMENT STRATEGY

General remarks:

It is hard to overestimate the importance of a well-executed international cyber 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 telecommunications 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.

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 and the ease of data transfer globally that necessarily make any viable cyber 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 a cyber engagement strategy, including those pertaining to cyber security, such as the Telecommunications Security Sector Reform (TSSR), data retention legislation 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 of 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 social change. Consequently, an ongoing dialogue between all stakeholders including the general public will be imperative for the effectiveness of a cyber strategy.

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

- Increased cyber literacy, especially in our key trading partner countries; and
- Improved international coordination and development of effective enforcement mechanisms at an international level.

In the following, we seek to provide high-level responses to some of the questions raised by the Department of Foreign Affairs and Trade. Our comments will focus on the first six questions as the remaining four questions appear to address sub-issues contained within the first six questions.

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

Q1: What are Australia's international interests in cyberspace? What are we doing well? What should we do differently? How can we do better?

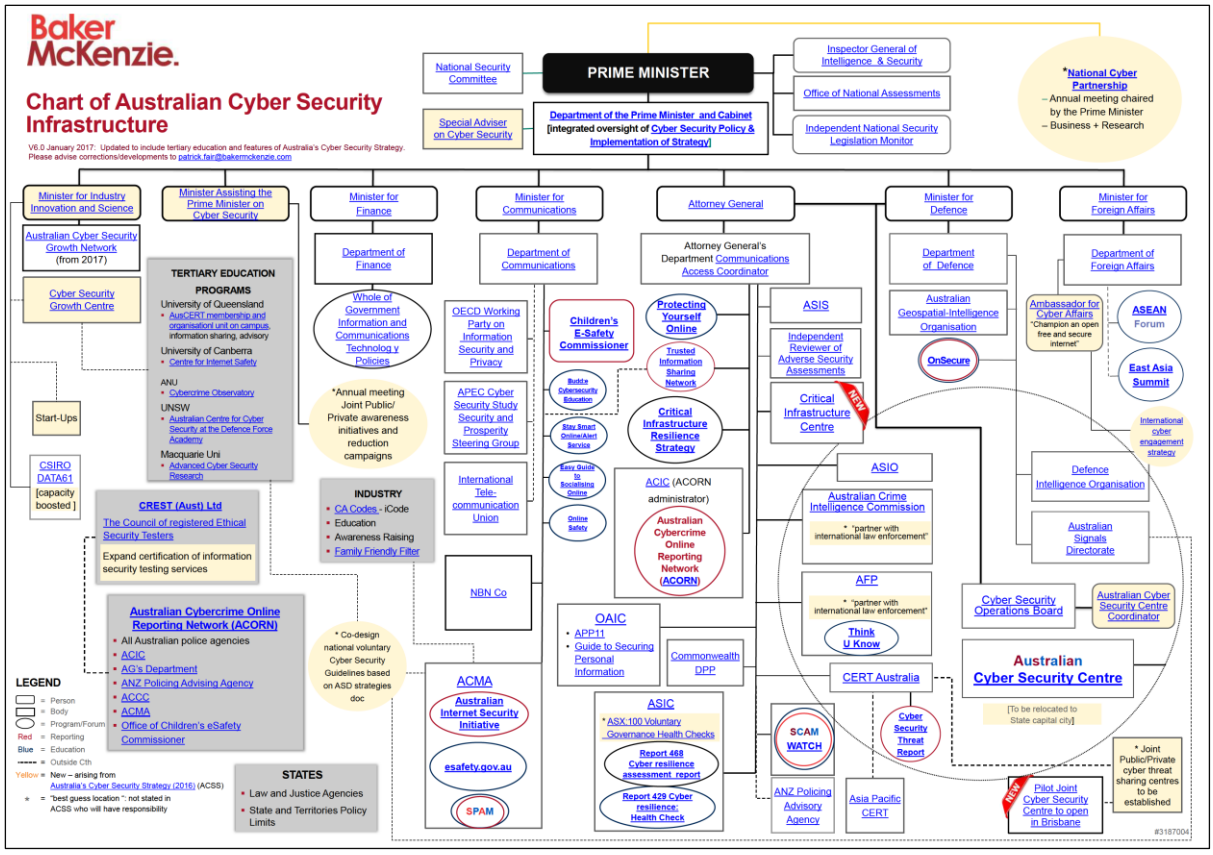
Q2: What does an ideal international cyberspace environment for Australia comprise?

Q5: What steps can we take to maximise trade and investment and expand commercial opportunities for Australian businesses, especially in the field of cyber security?

Q6: How can our international cyber engagement best support a free, open and secure Internet?

Current national cyber engagement landscape

As the below diagram highlights, the Australian cyber security landscape is characterised by a wide diversity of Government departments and agencies with partly overlapping and intersecting interest in or portfolio responsibilities relating to cyber security. These departments/agencies address a multitude of different stakeholders, e.g. telecommunications network operators, businesses across all sectors, the general public, etc. It appears that a better understanding of the precise roles and responsibilities of each of those, improved coordination of the current spread of agencies and programs and the creation of a single national point of access to Government's cyber security agencies would be likely to increase efficiencies and to deliver a clearer message to all stakeholders.



Note that the chart above only lists cyber security-related organisations and initiatives but does not include any other cyber-related Government organisations. While we do not

have access to a similar chart regarding the overall cyber-related activities by Government agencies, it is likely that a similarly complex picture may arise.

It is also likely that this cyber security landscape may make the pursuit of a unified and effective overall cyber strategy on a national level rather difficult and is likely to even more impede the development and effective and efficient execution of an international cyber engagement strategy.

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/fostering of open technological standards and a coherent (and timely) approach to the proliferation of the internet of things (IoT) immediately come to mind in this context.

Cyber literacy:

Importantly, any cyber framework ought to centre around the creation of a cyber literate nation. Individuals and businesses alike must understand the continuously changing requirements of the cyber world and adopt cyber security measures as part of their daily routine, lifestyle and business practices. Equally, industry and academia must ensure that cyber specialist resources are meeting national demand (in quality and quantity).

It is essential that individuals and particularly small businesses are being educated on the basics of IT functionality and security. A concerted coordinated effort is required to achieve high levels of awareness, education and implementation of security measures. Industry contends that the diverse array of education and awareness initiatives across federal and state agencies is not conducive to achieving this aim. It is recommended that, in close cooperation with Industry, a strategy be developed that analyses the key targets of educational initiatives, focuses the messaging and activities of each program accordingly and ensures a coordinated delivery. Overseas programs and the lessons that can be learned from those ought to be canvassed.

As we rapidly move toward an environment of IoT, the challenge of good cyber awareness, literacy and ultimately security equally moves from being a must for businesses to being imperative for all individuals in Australia who will own or operate an ever-increasing number and variety of smart devices, computers, consumer electronics, etc. Industry firmly believes that a coordinated Government-led education campaign is required to push and actively promote the safe(er) use of social media, email and the internet. Currently, Government initiatives like SCAM and the Stay Smart Online Alert Service go in this direction, however, they require individuals to actively search for information and subscribe rather than pushing information out to the general public. There is a role for Government to foster an instinctive understanding of the general public that the pervasiveness of telecommunications in general and the IoT in particular necessarily mean that cyber security is part of daily life and routine as much as road safety, environmental consciousness and healthy lifestyles ought to be. Such efforts must include a far greater awareness that stronger password protections for any sort of devices connected to the internet will be required in order to protect individuals' privacies from intended or accidental intrusion.

National and international standards and cooperation:

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 the staging post for phishing or other forms of fraud and deception online.

Therefore, we support 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 of threats 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, e.g. 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 the Defence level Common Criteria (CC). The provision of an independent validation for vendor product security claims, similar to the UK Government's Independent CESG Claims Tested Mark (CCTM) could be investigated. This validation essentially paralleled the CC EAL2 (claims test) – but at a realistic Industry/eGov/CNI level, rather than having to apply Defence criteria. Another part of this validation is the Certified Product Assurance (CPA) which paralleled the CC EAL3 (incorporating design, production, supply evaluation criteria). Key requirements of such validation programs are clear and trusted independence, effective costing for vendors and efficient and reliable turnaround times.

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.

Device security:

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. Given that 30 to 75 billion devices are forecast to be connected to the internet by 2020[3], with those devices often playing absolutely vital roles in everyday life, it is imperative that global device security standards are being developed and rigorously enforced by the responsible national agencies.

Opportunities for Australia

While cyber security poses challenges for Australia, we can see opportunities for Australia to become best-in-class and a world leader in identifying and managing cyber security threats and education campaigns. However, such opportunities will only arise on the back of a single cohesive, collaborative nation-wide approach to cyber security that is embraced by Government, industry and the public. Given the fragmented and at times uncoordinated approach to cyber security, Industry fears that Australia is not positioning itself to fulfil

[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.

[3] http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10

aspirations of best-practice and becoming an exporter of cyber security-related goods and services. Seizing these opportunities not only requires a more coherent and efficient national approach to cyber security but also active Government involvement at an international level.

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.

As it stands today, the world's population generates an estimated 2.5 quintillion bytes of data per day (about 10 million blue ray disks) and 90% of data in the world has been created in the past two years alone[4]. In addition to the already existing trend of creating ever more data, the proliferation of the IoT with an estimated 30 to 75 billion devices connected to the internet in 2020[5] and the advancements in artificial intelligence will hugely add to the data volumes generated in the near future.

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 still without regular or no access to the internet, a well-designed international cyber engagement strategy would provide a useful blue-print 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.[6] 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.

[4] https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html
[5] http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10
[6] Andrew Burt, "Virtual sovereignty can help govern our data", 6 February 2017, Financial Times

While the APEC Privacy Framework might be considered an early (and potentially outdated) step in the right direction in the sense that it constitutes an attempt to approach data privacy from a multi-national perspective, it appears that it may not have found the application, in particular developing member countries, that was hoped for and, importantly, it does not contain meaningful enforcement mechanisms or requirements. Critics of the Framework also argue that the standards it sets are significantly too low.[7]

In contrast, the European Union's General Data Protection Regulation (GDPR), appears to set much higher standards but is being criticised for being overly onerous and an impediment for innovation, especially for big data and the IoT.[8]

The above highlights the key issue to be considered when designing data and privacy frameworks, i.e. 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, Industries believes 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.

Q3: Which countries matter most to Australia's international cyber interests? Why and in what ways? How should we deepen and diversify key relationships?

Q4: Which regional and global forums and organisations matter most to Australia's international cyber interests? How should we support and shape them? How can we maximise influence?

We identified a number of 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.

Industry 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.

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

[7] Graham Greenleaf, "Five years of the APEC Privacy Framework: Failure or promise?", University of New South Wales
8 https://itif.org/publications/2016/04/14/new-eu-data-regulation-takes-digital-economy-two-giant-steps-backward-says

- Global Forum on Cyber Expertise
- Global Conference on Cyberspace
- Commonwealth Telecommunications Organisation

Regional Fora

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

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. 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.

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 international cyber 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 and that national structures ought to be more conducive to effective engagement on an international level.

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.

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