Australian Chamber of Commerce and Industry

Inquiry into the trade system and the digital economy

Submission to the Joint Standing Committee on Trade and Investment Growth
February 13, 2018

Digital economy, disruptive technology and Australia's trade architecture and regulatory system

There is no such thing as the "digital" economy. We need to recognise that there is only the economy in a digital world. Technological change is a constant but it is increasing and will be disruptive to traditional ways of doing things, including the global trade in goods and services.

Australia needs dynamic policy settings that recognise that the increasing availability of access to cloud based computing, high speed broadband, additive manufacturing (3D printing) and the internet of things will all challenge our previous thinking.

Envisaging disruption

Australia is part of a world where technology will increasingly allow goods and services to be provided in a digital form. This will impact on everything from accounting services to ice-cream, from tourism to entertainment. Consumers are demanding experiences, goods and services when and where they want, at low cost. These things could be delivered from any location around the world. As such the historic notion that goods and services come from a country, and that national Governments will be able to control them, will be increasingly challenged.

3D printing advancements will increasingly allow consumers to order personally tailored goods from international suppliers outside of the historic physical goods trading methods. This in turn will interrupt traditional customs functions and challenge border security.

Rigid structures like taxation, regulation and the notions of "work" and "jobs" will come under increasing pressure.

Policy needs to respond appropriately.

Trade modernisation

The Australian Government has already embarked on a process of trade modernisation and the Australian Chamber participates in this through membership of the National Committee on Trade Facilitation. The Government has recognised that there are opportunities for significant improvement in the way our trade in goods is managed. Historically, information has been required by border agencies to manage export controls and importing requirements. This same information is also often required by the commercial sector and it is currently entered and rekeyed many times. This can be streamlined with technologies like distributed ledger technology and improved risk based systems, rather than the Government needing to receive and assess this information in hard copy.

Just as these systems can improve the efficiency and reduce costs for information sharing, they also work in the same way for distribution of misinformation. Hence the opportunities for corrupt or malevolent purposes also need to be carefully considered. While there is a lot of excitement about blockchain, when it is used for the purpose of information sharing there is need for trusted "oracles" to authenticate information before it enters the ledger to ensure it is correct. This is a historic function of business chambers as a trusted partner of both commercial industry and Governments in similar systems like origin certification.

Chambers of commerce have been leaders in digital trade for many years. The system supporting international traders to comply with the origin requirements of international trade has been available in digital form for over a decade. Third party document preparation services have been offering 24/7 online digital services for many years and Chambers provide the "Government stamp" certification. This is vital to international trade through electronic means, which occurs at a rate of more than one per minute across Australia. However, Governments, both in Australia and around the world, continue to insist on paper based hard copy presentation of the resulting certificate of origin.

The Australian Chamber has recommended that the Department of Foreign Affairs and Trade (DFAT) seek a "digital by default" approach in modern trade agreements for documentary requirements, including evidence of origin. This will support importers when they seek to cross borders and comply with national market entry terms, as well as for the subsequent verification audits undertaken by Governments. To support advancement in this area the Australian Chamber has created *Chamber EDGE*, a new innovative platform. *Chamber EDGE* provides even greater functionality to both the commercial and regulatory sectors, supporting international trade documentation management and compliance.

The Australian Chamber recommends trade policy embrace likely future trends and ensure that regulatory requirements are fit for purpose to ensure innovation is encouraged. Technologies currently being trialled include distributed ledger technology to support financial services in trade and contractual performance, along with efforts to support consumer desires for provenance authenticity.

Port Community Systems – logistics and supply chains

The World Bank's *Doing Business* yearly report records the time and cost associated with the logistical process of exporting and importing goods in their 'Trading Across Borders' measure. In the Doing Business 2018 report, Australia was ranked 95th in the world for this measure (down from 27th in 2010)[i]. The time and costs associated with border crossing impact our national competitiveness and the ability of our internationally focussed businesses to engage in global markets.

Australia's land logistics management is an opportunity for dramatic efficiency improvements if transparency and big data can be harnessed. The Chamber of Commerce in WA undertook a study of possible improvements if Australia adopted a "Port Community System (PCS)" approach in the integration of our logistics and supply chains. PCS is an electronic platform which connects the multiple systems operated by a variety of organisations that make up a seaport, airport or inland port community. This study identified that there are over 120 transactions required to support the life cycle of a container through import and export involving over 750 pieces of information, of which over 300 were duplicated. The use of PCS would create efficiencies in this laborious process.

Internet creates new trade opportunities

Internet access and mobile technology is an enabler for regional communities and disadvantaged groups. The Australian Chamber has been working with DFAT on digital literacy and empowerment as a means to assist Women's Economic Empowerment[ii] in the Indian Ocean rim. Such technologies allow disadvantaged and regional communities to overcome many constraints to their wellbeing. The Vodafone Foundation's report[iii] found that mobile technology boosts economic

development through job creation and greater productivity and efficiency. This works in two directions: enabling people to connect to the world for improved information and international commercial engagement through both buying and selling.

Access to high speed internet is also an essential tool in modern international trade. Innovative and skilled Australians can provide goods and services to global markets, but we need to be able to do this at the appropriate speed and cost. Equally Australians increasingly buy services from the world, placing pressure on traditional retail operations. Australia needs to have world class enabling technology in order to take advantage of global opportunities that result from economic advancement around the world.

The digital economy and a cautionary tale

While there is a lot of opportunity and excitement about where the digital economy might lead, we would be wise to also consider that some scenarios would be extremely disruptive. For example, Asia's success over the past 50 years has been due to mobile capital taking advantage of low cost labour, reducing manufacturing conducted in advanced economies. With advances in robotics, artificial intelligence and other technologies that can perform the roles of people in repetitive tasks, this advantage may not continue. The same mobile capital may well come back "onshore" to the main target economies with new production systems that have the same, or better, efficiencies.

This could mean that, unless there is also continual structural adjustment in developing economies, they risk being caught in the middle income trap. As Australia relies on the economic advancement of these countries, particularly in our key areas of comparative advantage (food, fibre, resources, education and tourism), then our economy will also be pressured to change. Our economic policies need to be nimble and responsive to the impacts of rapid technological changes occurring around the world.

Australia itself will also need to make adjustments to our regulatory environment as we increasingly compete on the international stage. The need for internationally competitive taxation and workplace relations schemes has become more important than ever.

Cyber resilience and the Australian business sector

Targeted government approach

The Australian Chamber recommends consolidation of the various cyber security initiatives currently operating through various Australian Government agencies to avoid unnecessary duplication of efforts, increase effectiveness of response and avoid confusion. In the event of a cyber security incident, both the general public and Australian businesses would find it difficult to understand who to contact for help or notification. A refresh in the communications to the public and industry on cyber security initiatives would also be beneficial.

A quick search of Australian Government cyber security initiatives or resources yields the following results:

- Australian Cyber Security Centre (Attorney-General and Minister for Defence)
- Cyber Resilience Taskforce (Department of the Prime Minister and Cabinet)
- Australian Signals Directorate (Department of Defence)
- Computer Emergency Response Team (Attorney-General's Department)
- Australian Cyber Security Growth Network (Department of Industry, Innovation and Science)

- Australian Cybercrime Online Reporting Network (Australian, State and Territory governments)
- Stay Smart Online (part of Computer Emergency Response Team)
- Trusted Information Sharing Network (Attorney-General)
- OnSecure (Department of Defence)

State and Territory Governments have also implemented their own cyber security initiatives. While these initiatives show that Australian, State and Territory Governments are aware of the significant and serious impact a cyber threat can have on Australia, the sheer number of these initiatives creates vulnerabilities in Australia's cyber resilience.

The Australian Government should be vigilant about possible weaknesses in the digital ecosystem, being both proactive and reactive to cyber threats. In the event of a cyber security incident, having access to timely and complete information about the threat is vital in order to deploy appropriate mitigation strategies. This is necessary for both the Australian Government and Australian businesses to deploy the best safeguards for particular cyber attacks.

Given the number of current cyber security initiatives in place it is unlikely any one Australian Government area will have access to all available information in the event of a cyber threat, particularly as it is unclear which Australian Government agency would co-ordinate information gathering in the event of a cyber attack. This makes it quite difficult for Australian businesses to know who they should contact to better understand the magnitude of the cyber threat.

Collaborative networks increase cyber resilience

The Australian Chamber continues to recommend increased collaboration between the public and private sectors in the area of cyber security. In order for Australia to have a thriving and secure digital economy, it is essential that Australia develops its cyber security capabilities. The Australian Chamber recognises that there have been some positive steps in the right direction with the establishment of the Joint Cyber Security Centres and recommends the Australian Government continue to collaborate closely with the private sector, research organisations and universities to enable better detection, elimination and awareness of cyber security threats.

This could include, for example, sharing cyber security threat information through networks and expanding the Australian Cyber Security Centre. These collaborative networks will also enable Australian businesses to take advantage of economic opportunities that may arise in the cyber security sector, which is estimated to be currently worth over $100 billion.[iv]

Having collaborative cyber security networks that are clearly established, and are able to be identified by businesses, has been noted as a key proactive response to cyber threats.[v] The Australian Chamber recommends clear and secure communication channels be set up between private sector enterprises, government agencies and research institutions for the purpose of sharing information on cyber security threats. Effective information sharing will help contain the spread of cyber threats.[vi] Importantly, the methods used to share information should be constantly reviewed to ensure it is effective and adaptable to the constantly changing nature of the digital ecosystem.

Information sharing about cyber security threats also assists in creating strong cybersecurity foundations for organisations. Security intelligence helps organisations protect themselves both from internal and external cyber threats.[vii] Given cyber crime costs organisations, on average, US$11.7 million[viii] it is important that organisations are able to securely and safely share cyber security information to help ensure their safeguards are appropriate. As the sophistication of cyber security threats has increased[ix], many organisations are increasingly turning to security intelligence to better understand whether their existing cyber security safeguards are sufficient.

Communicating to industry and the public about cyber security threats

The Australian Government is far more likely to have access to broad-ranging information about cyber security threats due to having access to both industry and security agency information. This provides visibility of the whole cyber security landscape.[x] Consequently the Government should seek to focus its attention on its national communication channels so that the public and industry have no doubt as to where to go for information and assistance.

---

[i] The World Bank, Doing Business: Trading across borders http://www.doingbusiness.org/data/exploretopics/trading-across-borders
[ii] The Australian Chamber of Commerce and Industry, IORA: Women Mean Business https://www.australianchamber.com.au/initiatives/iora-women-mean-business/
[iii] Vodafone Foundation, Connected Women: How mobile can support women's economic and social empowerment, March 2014 https://www.vodafone.com/content/dam/connectedwomen/pdf/VF_WomensReport_V12%20Final.pdf
[iv] Australian Government, National Innovation & Science Agenda – Cyber Security Growth Centre: https://www.innovation.gov.au/page/cyber-security-growth-centre
[v] Cyber Resilience in the Digital Age, World Government Summit and NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies, ENISA (Nov 2016)
[vi] World Economic Forum, Cyber Resilience: Playbook for Public-Private Collaboration (Jan 2018)
[vii] Ponemon Institute and Accenture, 2017 Cost of Cyber Crime Study: Insights on the Security Investments that make a Difference
[viii] Ponemon Institute and Accenture, 2017 Cost of Cyber Crime Study: Insights on the Security Investments that make a Difference
[ix] Kim-Kwang RaymondChoo, The cyber threat landscape: Challenges and future research directions, Computers & Security (Nov 2011), Vol. 30, Issue 8, pages 719-731
[x] World Economic Forum, Cyber Resilience: Playbook for Public-Private Collaboration, January 2018