
AUSTRALIA'S
INTERNATIONAL
CYBER ENGAGEMENT
STRATEGY

Australian Government

ISBN

ISBN 978-1-74322-412-0 Australia's International Cyber Engagement Strategy (PDF)
ISBN 978-1-74322-413-7 Australia's International Cyber Engagement Strategy (Book [softcover])
ISBN 978-1-74322-414-4 Australia's International Cyber Engagement Strategy (webpage)

Attribution

This publication should be attributed as follows: Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*, October 2017

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the *It's an Honour* website: http://www.itsanhonour.gov.au/coat-arms/.

Website

http://www.cyberaffairs.dfat.gov.au

Contact

Enquiries about this document are welcome and should be directed to:

Cyber Policy Section
Department of Foreign Affairs and Trade
RG Casey Building, John McEwen Crescent
Barton ACT 0221

CONTENTS

FOREIGN MINISTER'S FOREWORD 4

INTRODUCTION BY THE AMBASSADOR FOR CYBER AFFAIRS 6

AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY AT A GLANCE 8

EXECUTIVE SUMMARY 10


DIGITAL TRADE 12


CYBER SECURITY 22


CYBERCRIME 32


INTERNATIONAL SECURITY & CYBERSPACE 44


INTERNET GOVERNANCE & COOPERATION 56


HUMAN RIGHTS & DEMOCRACY ONLINE 64


TECHNOLOGY FOR DEVELOPMENT 70


COMPREHENSIVE & COORDINATED CYBER AFFAIRS 82

ANNEXES 89

Foreign Minister's Foreword

We live in the most interconnected era in human history. Instantaneous communications, transactions, and access to information keep our economies growing, infrastructure operating, governments working and people in touch. Technology will continue to fundamentally change the way we live, work and relate to one another.

The borderless nature of cyberspace means international cyber issues present opportunities and challenges for all Australians, every day.

Digital trade, cyber-enabled intellectual property theft, technology for development and operations to influence elections are some of the ways cyber affairs permeate our international conversations.

The *2016 Cyber Security Strategy* committed to expanding on how Australia will attain global responsibility and influence in cyberspace.

Now, more than ever, we must engage with the international community as exciting possibilities emerge, critical debates unfold and global rules are agreed.

Australia's first *International Cyber Engagement Strategy* states Australia's comprehensive international cyber affairs agenda. It sets a clear vision of Australia's interests and objectives in cyberspace over the next three years.

Reflecting Australia's broad view of cyber affairs, this Strategy establishes a whole-of-Government approach across seven key themes: Digital Trade, Cyber Security, Cybercrime, International Security, Internet Governance & Cooperation, Human Rights & Democracy Online and Technology for Development. The Strategy is supported by a practical action plan.

The *Foreign Policy White Paper*, currently under development, will reiterate our understanding of the significant and growing importance of cyber issues to Australia's foreign policy. It will also chart a course to position Australia for opportunity, while managing the risks of our increasingly interconnected world.

Our international cyber engagement protects Australians and promotes our interests. It positions us to harness opportunities and increase our cyber resilience. An open, free and secure Internet drives economic growth, enhances our national security and fosters international stability.

Australia remains committed to a peaceful online environment.

The activities of states in cyberspace have implications for us all. Cyberspace is not an ungoverned space. Just like in the physical domains, states have rights but they also have obligations. Existing international law applies to states' conduct in cyberspace, complemented by agreed norms of responsible state behaviour.

Increasingly, states are testing the boundaries of what is and isn't acceptable in cyberspace. Australia will cooperate with its international partners to deter, mitigate and attribute malicious cyber activity by criminals, state actors and their proxies, including those that seek to interfere in the internal democratic processes of states.

Australia's cyber affairs agenda is global in perspective and regional in focus.

As a responsible contributor to the international community, we have a platform to engage on cyber policy issues within global forums. Strong participation in global cyber cooperation efforts benefits Australia's national and economic interests. It also positions Australia to take a leading international role in shaping the future of cyberspace.

The Indo-Pacific region presents significant digital opportunities and complex cyber challenges. It is home to some of the most advanced digital economies as well as countries whose digital development is still in its early stages. It is here, in the Indo-Pacific, that Australia can best leverage our cyber capacity building resources to support and open, free and secure Internet.

Digital technologies are profound enablers of sustainable development and economic growth.

Australia will work to improve connectivity and access to the Internet across the Indo-Pacific. We will encourage the use of resilient development-enabling technologies for egovernance and digital delivery of services. We will also support entrepreneurship, help develop a digital ready workforce and promote our region's further integration into the global market place.

This Strategy sets out Australia's plan to promote confidence in the online environment, increase economic opportunities, reduce losses attributable to cybercrime, minimise the risks of strategic miscalculation in cyberspace, promote multi-stakeholder Internet governance, protect human rights online and deliver sustainable development outcomes.

I look forward to engaging with governments at home and abroad, the private sector, civil society and academia to enhance the prosperity and security of Australia, our region, and the world.

The Hon Julie Bishop MP
Minister for Foreign Affairs

4 October 2017

Introduction by the Ambassador for Cyber Affairs

Cyber affairs play a significant role in Australia's international relations with other countries. While once a technical niche issue, cyber affairs is now a strategic international policy issue.

Thanks to cyberspace, the connections between governments, businesses, communities and individuals are more complex than ever before.

As the complexity of cyberspace grows, it demands increased international attention, cooperation and creativity.

This Strategy sets an ambitious agenda across the full spectrum of cyber affairs. Framing Australia's international cyber interests through this comprehensive lens empowers us to see the big picture of the dynamic cyber landscape.

Australia's interests in cyberspace are diverse and interconnected: from capturing the economic prosperity promised by digital trade and technology enabled-development, to securing Australia from the threat of cybercriminals and preserving stability in cyberspace.

Growth of disruptive business models supported by digital technologies present exciting opportunities for Australian businesses. Government and the private sector therefore have a mutual responsibility and interest in maximising the opportunities and mitigating the risks of the online world.

Australia's vision of an open, free and secure cyberspace and our ambitions across the broad spectrum of cyber affairs are impossible to achieve alone. All of our efforts, both globally and regionally, will be delivered in partnership. We will combine the unique and complementary skills of other countries, the private sector, civil society and the research community.

International cyber issues are constantly evolving and Australia's approach to international cyber engagement must reflect this. Frequent review of Australia's approach to cyber affairs will ensure Australia continues to adopt the most effective means to achieve our goals in cyberspace.

Harnessing the opportunities of the digital age and mitigating risks is a shared challenge and a shared responsibility. My team and I look forward to working with you to advance and protect our collective interests in cyberspace.

Dr. Tobias Feakin
Ambassador for Cyber Affairs

4 October 2017

AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY AT A GLANCE

COMPREHENSIVE & COORDINATED CYBER AFFAIRS

Australia pursues a comprehensive and coordinated international cyber affairs agenda

- **Enhance** understanding of Australia's comprehensive cyber affairs agenda
- **Increase** funding for Australia's international cyber engagement activities
- **Coordinate** and prioritise Australia's international cyber engagement activities

DIGITAL TRADE

Maximise the opportunity for economic growth and prosperity through digital trade

- **Shape** an enabling environment for digital trade, including through trade agreements, harmonisation of standards, and implementation of trade facilitation measures
- **Promote** trade and investment opportunities for Australian digital goods and services

CYBERCRIME

Stronger cybercrime prevention, prosecution and cooperation, with a focus on the Indo-Pacific

- **Raise** cybercrime awareness in the Indo-Pacific
- **Assist** Indo-Pacific countries to strengthen their cybercrime legislation
- **Deliver** cybercrime law enforcement and prosecution capacity building in the Indo-Pacific
- **Enhance** diplomatic dialogue and international information sharing on cybercrime

INTERNATIONAL SECURITY & CYBERSPACE

A stable and peaceful online environment

- **Set** clear expectations of state behaviour in cyberspace
- **Implement** practical confidence building measures to prevent conflict
- **Deter** and respond to unacceptable behaviour in cyberspace

INTERNET GOVERNANCE & COOPERATION

An open, free and secure Internet, achieved through a multi-stakeholder approach to Internet governance and cooperation

- **Advocate** for a multi-stakeholder approach to Internet governance that is inclusive, consensus-based, transparent and accountable
- **Oppose** efforts to bring the management of the Internet under government control
- **Raise** awareness across the Indo-Pacific of Internet governance issues and encourage engagement of regional partners in Internet governance and cooperation discussions

HUMAN RIGHTS & DEMOCRACY ONLINE

Human rights apply online as they do offline

- **Advocate** for the protection of human rights and democratic principles online
- **Support** international efforts to promote and protect human rights online
- **Ensure** respect for and protection of human rights and democratic principles online are considered in all Australian aid projects with digital technology components

TECHNOLOGY FOR DEVELOPMENT

Digital technologies are used to achieve sustainable development and inclusive economic growth in the Indo-Pacific

- **Improve** connectivity and access to the Internet across the Indo-Pacific, in collaboration with international organisations, regional governments and the private sector
- **Encourage** the use of resilient development-enabling technologies for e-governance and the digital delivery of services
- **Support** entrepreneurship, digital skills and integration into the global marketplace

CYBER SECURITY

A strong and resilient cyber security posture for Australia, the Indo-Pacific and the global community

- **Maintain** strong cyber security relationships with international partners
- **Encourage** innovative cyber security solutions and deliver world leading cyber security advice
- **Develop** regional cyber security capability
- **Promote** Australia's cyber security industry

EXECUTIVE SUMMARY

Australia's international cyber engagement champions an open, free and secure cyberspace. Through comprehensive and coordinated engagement on cyber affairs, we will maximise opportunities for economic growth and prosperity through digital trade. Australia will cooperate internationally to reduce the risk of cybercrime and promote peace and stability in cyberspace. We will advocate for multi-stakeholder Internet governance and respect for human rights and democratic principles online. We will partner to foster good cyber security practices and encourage the use of digital technologies to achieve sustainable development, particularly in our region.

The digital technology revolution is fundamentally a story of prosperity. Increasingly, cyberspace acts as an economic enabler. Connectivity helps improve productivity and provides customers and the private sector with greater access to the global marketplace. Shaping an enabling environment for digital trade will deliver increased prosperity for Australia and enhance realisation of economic opportunity globally.

This progress is only possible if underpinned by sound cyber security. The spread of digital technologies creates profound economic opportunities but, at the same time, creates new vulnerabilities. Individuals, the private sector and governments around the world face an evolving array of cyber threats. Governments and the private sector working together to develop a strong cyber security posture is an essential prerequisite to ensuring we can all safely capitalise on the benefits of increasing connectivity. As part of this effort, Australia will encourage innovative cyber security solutions and deliver world leading cyber security advice.

Improving cyber security is an important way of mitigating the risk of cybercrime. Left unchecked, criminal use of the Internet threatens to undermine the economic opportunity offered by the digital domain. Like cyberspace, cybercrime is not confined by geographic borders.

As such, Australian individuals, the private sector and government can be exposed to threats emanating from other countries. Working collaboratively with international partners and helping countries in our region improve their capacity to address cybercrime will improve prevention and prosecution of cybercrime worldwide.

It is not only criminals who threaten the online environment. Developments in cyberspace have created a new arena in which states can exert influence. The increasingly complex nature of the international landscape means that more and more actors now pursue strategic goals in the digital domain; some challenging the international rules-based order in the process. Australia is committed to a peaceful and stable cyberspace. We will cooperate with international partners to deter and respond to malicious cyber activity that endangers international peace, security and stability. Reaffirming the application of international law to cyberspace, adhering to norms of responsible behaviour in cyberspace and implementing confidence-building measures will shape cyberspace as a landscape for international cooperation and mutual benefit.

The private sector, civil society, academia, individuals and government are all important stakeholders in cyberspace. A multi-stakeholder approach to Internet governance, which places all stakeholders on an equal footing in Internet governance debates, best facilitates an open, free and secure Internet. Better multi-stakeholder cooperation domestically, regionally and internationally will preserve decentralised control of the Internet, allowing all voices to be heard when decisions over the policy and technical management of the Internet are made.

The promotion and protection of human rights and democratic principles online is crucial; human rights apply online as they do offline. The Internet itself has provided an unparalleled opportunity for online democratic participation and the promotion, protection and fulfilment of human rights. This contributes to lasting peace, security, freedom and dignity for all. Governments, the private sector, civil society and academia must continue to work together to uphold and defend human rights online, just as they do offline.

Beyond the realisation of human rights, connectivity and the uptake of digital technologies also act as a profound enabler of sustainable development and inclusive economic growth. Innovative uses of technology, entrepreneurial activities and the digital upskilling of workforces have seen economies transform and societies make great leaps in development. However, dividends of the digital age are currently not evenly experienced. Increasing connectivity and harnessing digital technologies safely will accelerate the attainment of sustainable development objectives, especially in regions, countries and populations where digital journeys are only just beginning.

Australia's International Cyber Engagement Strategy addresses the full breadth of these issues, from trade to cybercrime, from international security to international cooperation, and from human rights to sustainable development. Australia has adopted a comprehensive and coordinated approach to cyber affairs. We will achieve our objectives in cyberspace through cooperation, creative partnerships and practical action.

DIGITAL TRADE

AUSTRALIA'S GOAL:

Maximise the opportunity for economic growth and prosperity through digital trade

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- **Shape** an enabling environment for digital trade, including through trade agreements, harmonisation of standards, and implementation of trade facilitation measures
- **Promote** trade and investment opportunities for Australian digital goods and services

Digital technologies and the Internet are key drivers of economic growth and innovation. The digital economy has shifted from a niche sector to an essential part of the economy. The line between traditional goods and digital goods is blurring. The Internet makes it easier for consumers and businesses to trade goods, services and information around the world.

Digital trade is not just about buying and selling goods and services online, it is also the transmission of information and data across borders. It relies on the use of digital technologies to facilitate trade and improve productivity, for example through simplified customs procedures. While flows of information and data may not always be for profit, they are essential enablers of digital trade.

Nowhere is the potential for digital trade greater than in our region. For the first time, in 2017 more than 50 per cent of global Internet users were located in the Indo-Pacific. Yet, only 46.4 per cent of households in the Indo-Pacific were connected to the Internet in 2016, so there are vast untapped opportunities for digital trade. Successfully harnessing this opportunity promises economic growth for countries in the region as well as new market opportunities for Australian businesses.

However, this potential can only be realised if countries cooperate to establish an enabling environment for digital trade. Governments must work with the private sector and consumer groups to ensure digital trade policies and norms and rules foster economic growth and security. This work must be practical, evidence-based and consensus driven. It should be coupled with international efforts to expand participation in digital trade across the Indo-Pacific, which will grow markets for Australian businesses and broaden economic development opportunities for all.

Shape an enabling environment for digital trade

Australia is committed to actively shaping global rule-making on digital trade. Australia will advocate for global rules that support digitisation of trade-related practices, build trust and confidence in the online environment, and reduce barriers to digital trade.

Global trade rules should support existing global and regional norms, principles and guidelines. This includes those developed through the United Nations (UN), the World Trade Organization (WTO), the Organisation for Economic Cooperation and Development (OECD), the G20, APEC, and international standards-setting bodies such as the International Organisation for Standardisation. Australia engages in these multilateral forums to cooperate on practical steps that promote digital trade, sharing best practice, and addressing emerging policy issues.

ENABLE GREATER ACCESS TO GLOBAL MARKETS AND A MORE CERTAIN REGULATORY ENVIRONMENT

In addition to influencing trade rules through key international forums, Australia has included 'electronic commerce' chapters in 10 of its 11 concluded free trade agreements. Australia is currently pursuing commitments on digital trade in our bilateral negotiations with Indonesia, Hong Kong and Peru, and with countries participating in the negotiations for a *Regional Comprehensive Economic Partnership* and the *Trade in Services Agreement*.

International rules that facilitate the free flow of information and data across borders are also important for promoting digital trade. Data flows now have generated a greater impact on global gross domestic product growth than the global trade in goods. As customs duties on electronic transmissions may restrict the growth of online trade, Australia is committed to a permanent moratorium on customs duties on electronic transmissions.

DIGITAL TRADE IN THE WORLD TRADE ORGANIZATION

The World Trade Organization (WTO) is the key multilateral organisation governing international trade. Through its membership, Australia pursues commitments that improve market access for businesses and increase consumer choice, including in digital trade. Australia supports crucial WTO agreements on goods, services and intellectual property, including the *Agreement on Trade Facilitation (TFA)*. Australia also supports the adoption of agreements that encourage WTO members to take on further digital trade and trade facilitation commitments. These include the WTO *Information Technology Agreement* (ITA) and the *Telecommunications Reference Paper*.

Australia promotes trade enabling rules and the free flow of information. But we recognise the importance of allowing governments to respond to legitimate public policy concerns, including consumer and privacy protections.

Australia encourages international partners to do so transparently and with appropriate consultation (*see Support Transparency and Evidence-based Policy Positions, page 20*).

TABLE 1: This table outlines some of the key provisions Australia pursues in its trade agreements to enable digital trade. These objectives are general, may change in specific negotiations and are negotiated in the context that we are able to accommodate our policy sensitivities, including in regard to health, environment, consumer and privacy protections, and security.

Provision	Description
Paperless trading	Countries should provide for online availability of import and export documentation and electronic submission of those documents
Electronic authentication	Countries should not deny a signature on the basis it is in electronic form, and should adopt a flexible approach to authentication technologies
Online consumer protection	Countries should provide the same protections for online consumers as they do for any other consumer
Online protection of personal information	Countries should adopt or maintain a legal framework to protect the personal information of electronic commerce users from unauthorised disclosure
Unsolicited commercial electronic messages (spam)	Countries should adopt or maintain measures to allow consumers to opt out of receiving unwanted commercial messages (for example email and SMS) from various sources and to provide that businesses only send such messages with the expressed or inferred consent of the consumer with the source of the messages identified
Customs duties on electronic transmissions	Countries should continue the practice of not applying customs duties to electronic transmissions
Domestic regulatory frameworks / domestic electronic transaction frameworks	Countries should adopt or maintain legal frameworks consistent with the principles of the UN Commission on International Trade Law (UNCITRAL) *Model Law on Electronic Commerce (1996) and the UN Convention on the Use of Electronic Communications in International Contracts (2005)*

Provision	Description
Localisation of computing facilities	Countries should not require businesses operating in their territory to locate computing facilities (including computer servers and storage devices for processing or storing information for commercial use) within the country's borders
Cross-border transfer of information by electronic means	Countries should allow cross-border transfers of information by electronic means
Disclosure of source code	Countries should not require the transfer of or access to mass-market software source code as a condition for the import, distribution, sale or use of software
Cooperation	Governments should cooperate on areas of mutual interest in digital trade including on cyber security matters
Elimination of customs duties on technological products	Countries should eliminate customs duties on technological business and consumer products through participation in the *Information Technology Agreement*, or products covered by that agreement
Trade facilitation commitments	Countries should continue to implement commitments made in the *Trade Facilitation Agreement* and endeavour to build on those commitments to ensure the efficient movement of goods across borders
Commitments on performance requirements	Countries should not require technological transfers as a condition of investing in another country

AUSTRALIA WILL:

1.01 Advocate for further digital trade liberalisation and facilitation through free trade agreements and participation in the WTO, OECD, APEC and G20

HARMONISE STANDARDS

An enabling environment for digital trade requires clear standards. Australia's interests in the development of standards is discussed in the *Cyber Security chapter*. However, developing these standards in isolation will not achieve the desired outcome. Standards need to be harmonised between countries to improve the conditions for global digital trade by making it easier to do business across borders.

Just like global trade rules, international standards need to be industry-led and technology-neutral. In particular, Australia supports the development of globally interoperable Internet standards and associated reference architecture, as well as *ISO 27000 Information Security Management Systems* standards.

To reduce the need for burdensome regulation, Australia also supports increased cooperation between national standards bodies and regulatory agencies across the Indo-Pacific. Australia will further reduce barriers to trade by proactively harmonising standards and promoting international trade across the Indo-Pacific.

AUSTRALIA WILL:

1.02 Support capacity building projects in the Indo-Pacific to encourage the harmonisation of international standards for digital goods, building trust and confidence in digital trade

TRADE FACILITATION

Australia supports practices that improve the efficiency of trade conducted electronically, including through the use of digital technologies, such as paperless trading and electronic authentication (*see Table 1, page 15*). Australia will continue to support trade facilitation in key international forums. This includes exploring the trade-enabling and cost reduction potential of emerging technologies such as Blockchain. Australia also recognises that strong cyber security builds trust in cyberspace and facilitates digital trade.

AUSTRALIA WILL:

1.03 Oppose barriers to digital trade and advocate for implementation of the WTO Trade Facilitation Agreement through bilateral representations and involvement with WTO committees and councils, APEC and the G20

1.04 Design and trial an electronic Secure Trade Lane with New Zealand to provide benefits for trusted traders in both countries

SUPPORT REGULATORY COOPERATION

Regulators are responsible for ensuring fairness and transparency in markets and establishing an enabling environment for digital innovation. Cooperation between regulators is important for supporting digital trade. It can build trust and overcome uncertainty and other barriers to the growth of digital trade. Regulatory cooperation in the financial technology sector is already underway and has yielded early successes (*see International Efforts of the Australian Securities and Investment Commission, page 19*).

INTERNATIONAL EFFORTS OF THE AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (ASIC)

Within the Financial Technology (FinTech) sector, ASIC has formal innovator business referral arrangements with its counterparts in the United Kingdom, Singapore, Malaysia, Japan and Hong Kong. ASIC also has information sharing agreements with Kenya's Capital Markets Authority and ASIC's Indonesian counterpart, Otoritas Jasa Keuangan (OJK). These agreements enhance Australian capacity building programs in the region, specifically the *Australia-Indonesia Partnership for Economic Governance*, through direct regulator-to-regulator transfer of knowledge and experience. ASIC has also provided assistance via multilateral programs such as the *Mekong Business Initiative* and the APEC *Financial Regulators Training Initiative*, and through direct participation in the inaugural FinTech Regulation Bootcamp held in Singapore in October 2016.

AUSTRALIA WILL:

1.05 Promote regulatory cooperation and coherence through Australia's bilateral exchanges, the Australian free trade agreement agenda, Aid for Trade activities, as well as engagement in APEC and G20

SUPPORT TRANSPARENCY AND EVIDENCE-BASED POLICY POSITIONS

Australia is committed to leading by example on stakeholder consultation and transparency in policy-making. Appropriate multi-stakeholder consultations help ensure well-targeted policy responses to the challenges and opportunities of digitisation. Australia will continue to hold regular consultations with industry on digital trade and invite submissions from the private sector when developing new digital trade rules. Similarly, Australia encourages other countries to consult with businesses when developing new trade laws and policies.

More work needs to be done to accurately measure digital trade. Understanding the current uptake of digital technologies by micro, small and medium enterprises, and the barriers to their digital participation, will better inform policy. Australia is committed to working towards internationally consistent and robust measurement of digital trade.

AUSTRALIA WILL:

1.06 Support public-private engagement on emerging digital trade issues in multilateral forums, including the Business 20 and the APEC Business Advisory Council

1.07 Support the G20, OECD and other international research to improve digital trade measurement and develop policy responses

1.08 Encourage transparency from bilateral partners on domestic legislation that could restrict trade, including through cyber policy dialogues

Promote trade and investment opportunities for Australian digital goods and services

Australia actively promotes its digital goods and services internationally to maximise opportunities for Australian businesses in the booming global digital economy. To attract foreign investment, Australia leverages its global reputation as a trusted and secure place to do business, with robust domestic safeguards, a well-developed services economy and a quality education system.

To maximise international digital trade opportunities for Australian businesses, Australia will develop a whole-of-Government digital economy strategy, led by the Department of Industry, Innovation and Science. Austrade will also create a practical guide for Australian companies exporting in the digital economy. These documents will be developed in close consultation with the private sector.

PRIVATE SECTOR ENGAGEMENT ON DIGITAL TRADE

The private sector is at the centre of Australia's digital trade efforts. To inform Australia's digital trade promotional activities, the Australian Government will consult closely with the private sector. In addition to consulting with large multi-nationals through APEC and the G20, the Ambassador for Cyber Affairs will establish industry consultations and workshops, including an Industry Advisory Group focused on Australia's international cyber engagement (*see the Comprehensive and Coordinated Cyber Affairs chapter*).

AUSTRALIA WILL:

1.09 Develop a guide to exporting in the digital economy, providing practical advice for maximising international opportunities for Australian businesses

1.10 Develop a national digital economy strategy, which will position Australia to embrace the opportunities presented by digital trade

CYBER SECURITY

AUSTRALIA'S GOAL:

A strong and resilient cyber security posture for Australia, the Indo-Pacific and the global community

TO ACHIEVE THIS AUSTRALIA WILL:

- **Maintain** strong cyber security relationships with international partners
- **Encourage** innovative cyber security solutions and deliver world leading cyber security advice
- **Develop** regional cyber security capability
- **Promote** Australia's cyber security industry

Cyber security provides the foundation for the achievement of Australia's entire cyber affairs agenda. Cyber security is an important theme of every part of this Strategy. This chapter addresses the specific activities that Australia undertakes internationally to achieve a strong and resilient cyber security posture for Australia, the Indo-Pacific and the global community.

The objective of strong cyber security is to enable access to online information by individuals, governments and businesses, while ensuring the information and the systems that underpin it are protected from unauthorised access, removal or change. This increases the trust and confidence of users, which will underpin continued investment in innovative technologies, driving continued economic growth.

Australia cannot act in isolation. Collaborative networks with international partners are critical to combatting global threats. Cyber security is strengthened by a dynamic domestic cyber security industry that is active internationally. This in turn will help grow Australia as a hub for international cyber security research and education. Australia's trusted international relationships will foster a readiness to share information and best practice, and cooperate to solve technical problems.

CYBER SECURITY

Cyber security encapsulates measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.

Maintain strong relationships with international partners

Engaging internationally to strengthen the collective cyber security of Australia, the Indo-Pacific and the broader global community is a key objective for Australia. The global nature of the Internet means that cyber threats emerging anywhere in the world can impact Australia. Our international engagement will seek to build Australia's knowledge and capabilities and to enhance the cyber security posture of international partners, particularly those with extensive economic, diplomatic and social links with Australia. By improving the cyber security of our partners, we strengthen our own cyber defences.

Sharing cyber security information with international partners builds strong collective understanding of threats. It also improves our combined ability to prevent, detect, analyse, respond, mitigate and recover from cyber security threats and incidents. Building trusted international cyber security threat sharing networks gives Australia and our partners the best possible chance of staying ahead of malicious actors.

Through the Australian Cyber Security Centre (ACSC), Australia engages with international cyber security organisations, law enforcement agencies and industry partners. This cooperatively develops our collective cyber resilience, and assists law enforcement agencies to investigate cybercrimes.

Computer Emergency Response Teams (CERTs) and cyber security centres around the world work to protect and respond to incidents affecting systems of national interest. Partners are able to build a trusted community where indicators of compromise and threat information are shared – preferably automatically. This ensures that all members of trusted information sharing networks are well-placed to take informed actions in their respective domestic contexts.

This cooperation is framed by Australia's suite of cyber policy dialogues with a range of international partners including China, India, Indonesia, Japan, New Zealand and South Korea.

THE AUSTRALIAN CYBER SECURITY CENTRE'S INTERNATIONAL CYBER ENGAGEMENT EFFORTS

The Australian Cyber Security Centre (ACSC) brings together cyber security capabilities across the Australian Government to enable a more complete understanding of sophisticated cyber threats, facilitate faster and more effective response to significant cyber incidents, and foster better interaction between government and industry partners. The ACSC engages with international partner organisations to share cyber threat information, to cooperate on operational responses to major cyber incidents and to work collaboratively on best practice mitigations.

Australia has established cyber security information sharing arrangements with a variety of strategic international partners across the public sector, private sector and research communities. These include bilateral agreements and memoranda of understanding, engagement between intelligence agencies, national cyber security centres, industry bodies, cyber security researchers, and participation in regional and international forums.

Australia will continue to strengthen and expand our network of strategic information sharing partners, both providing and receiving information to enhance the cyber security posture of Australia and the cyber security of our international partners. The establishment of Joint Cyber Security Centres and the relocation of the ACSC to a new purpose-built facility will facilitate improved collaboration and more integrated partnerships.

The ACSC through CERT Australia, Australia's national CERT, works closely with industry partners to protect domestic critical infrastructure and other systems of national interest. To facilitate this, CERT Australia has a number of key operational level relationships with bilateral partners and multilateral forums. Australia's international CERT relationships enable the trusted sharing of threat information and the joint development of tools and techniques to prevent, detect, analyse, respond, mitigate and recover from cyber incidents. This global CERT network supports the ACSC's capability to respond to cyber incidents and assists domestic industry partners to take proactive cyber security measures.

CERT Australia is committed to strengthening and expanding its network of CERT relationships in the Indo-Pacific and more broadly to secure Australia's critical infrastructure and other systems of national interest. Australia is committed to participating in coordinated global efforts to strengthen global CERT capacity – both sharing our expertise and learning from others.

While the structure, mandates and constituencies of national CERTs may differ, they also have many commonalities. They are operationally focused and staffed by cyber security professionals with the technical expertise to respond to cyber incidents. A key role for a national CERT is to be a main operational point of contact during an international cyber incident, assisting in the conduct of coordinated incident response.

International collaboration at this technical operationally focused level ensures the ACSC can perform incident response activities in Australia quickly and effectively.

ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM

The Asia Pacific Computer Emergency Response Team (APCERT) is a grouping of leading and national CERTs and Computer Security Incident Response Teams dedicated to the protection of national infrastructure in the Asia Pacific. It is just one example of economies collaborating to build collective incident response capability in order to prevent, detect, analyse, respond, mitigate and recover from cyber incidents. APCERT has an operational focus with objectives to help create a safe and reliable cyberspace in the Asia Pacific through global collaboration. CERT Australia currently chairs the APCERT Steering Committee and, with the other APCERT members, participates in an annual APCERT drill and other capacity building activities.

AUSTRALIA WILL:

2.01 Strengthen and expand Australia's strategic international cyber security information sharing partners and trusted networks

2.02 Strengthen and expand Australia's network of CERT relationships, especially in the Indo-Pacific

2.03 Be a prominent contributor to the APCERT community

Encourage innovative cyber security solutions and deliver world leading cyber security advice

ENCOURAGE INNOVATIVE CYBER SECURITY SOLUTIONS

Increasing connectivity, and the proliferation of devices connected to the Internet (the Internet of Things), highlights the importance of security as a fundamental driver in the design and delivery of information communication and technology (ICT) products, systems and services. Australians use digital products and services from all over the world. There is still much work to be done internationally to promote the development of ICT products, systems and services that are secure by design.

Cyber security experts in the ACSC engage with the leading innovators and technical experts in the ICT vendor community to share expertise. ACSC experts also promote cyber security as a fundamental element in the design of new products, systems and services. These partnerships inform cyber security technical advice produced by the ACSC, as well as improving the cyber security functionality within new products, systems and services.

Australia will continue the evaluation of the security of ICT products through the Australasian Information Security Evaluation Program's involvement in the Common Criteria Recognition Arrangement (*ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation*). We will also support the efforts of standards bodies, including work by Standards Australia (*see below*) on the *ISO/IEC 27000* series of information security standards.

STANDARDS AUSTRALIA

The development and application of international standards play a key role in improving the quality and cyber security of digital products, systems and services across the globe, and assist in protecting governments, business and consumers alike.

Standards Australia, as a member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), contributes to developing international standards. These standards are designed to enhance the security of information technology systems, networks and critical online infrastructures. This work is carried out through ISO's Technical Committees (TCs) and Joint Technical Committees (JTCs).

Australia's contribution in this area includes leading development of international standards for ISO/TC 307 Blockchain and other distributed ledger technologies. We also work with other ISO/IEC JTC One members on cloud computing and distributed platforms and information technology security techniques.

DELIVER WORLD LEADING CYBER SECURITY ADVICE

Australia produces world leading cyber security advice and best practice, which, if implemented, enhances the cyber security of individuals, businesses and governments. This includes the *Information Security Manual, Strategies to Mitigate Cyber Security Incidents* and its *Essential Eight*, as well as the *Stay Smart Online* guidelines for small businesses and individuals.

THE AUSTRALIAN SIGNALS DIRECTORATE'S ESSENTIAL EIGHT

ASD has developed the *Essential Eight* strategies to mitigate cyber security incidents. This framework provides helpful practices that organisations can implement in their everyday operations to improve their cyber security.

Through its international cyber security engagement and partnerships with the private sector, Australia will promote the adoption of best practice cyber security advice to raise the bar for international cyber security, enhancing the cyber resilience of our international partners.

As a first step, Australia will translate and publish ASD's *Essential Eight* mitigation strategies and its companion documents into the official languages of the 10 member states of the Association of Southeast Asian Nations (ASEAN).

AUSTRALIA WILL:

2.04 Promote cyber security as a fundamental input to the design and delivery of information and communication technologies products, systems and services

2.05 Support the development of international standards that improve cyber security and encourage harmonisation of standards for digital products

2.06 Publish translations of ASD's Essential Eight strategies and companion implementation documents in the official languages of ASEAN members

Develop regional cyber security capability

Australia is committed to assisting partners in the Indo-Pacific develop their capacity to address cyber threats, strengthen cyber security and combat cybercrime through the *Cyber Cooperation Program* (*see the Comprehensive & Coordinated Cyber Affairs chapter*). Increasing connectivity in the Indo-Pacific is a force for significant social and economic development and inclusion. However, increased connectivity also has the potential to expose the region to increased threats from malicious cyber actors.

Recognising the importance of cyber resilience, and with the understanding that not every country in our region has the capacity to establish a cyber security capability such as a national CERT, Australia will work with our Pacific neighbours to establish a Pacific Cyber Security Operational Network (PaCSON).

The PaCSON network will consist of technical experts from respective governments across the Pacific, and will be supported by other partners including not-for-profit organisations and academia. PaCSON will establish operational cyber security points of contact. It will empower members to share cyber security threat information; provide opportunities for technical experts to share tools, techniques and ideas; and be an enabler of cooperation and collaboration, particularly if a cyber security incident affects the region. Further, it is envisaged that PaCSON will provide members with a toolkit for cyber security incident response and assist with cyber security awareness raising activities across the Pacific.

AUSTRALIA WILL:

2.07 Work with regional partners in the Pacific to establish PaCSON

Promote Australia's cyber security industry

EXPORT AUSTRALIAN CYBER SECURITY SOLUTIONS

Australia is committed to growing a vibrant cyber security sector in response to the increasing domestic and regional demand for cyber security solutions. Australia has designated the cyber security sector as a key sector for export promotion. We are committed to increasing the number of Australian cyber security companies operating successfully in global markets.

Australia is collaborating with private sector partners, including the Australian Cyber Security Growth Network (AustCyber), to develop a deeper understanding of Australian cyber security capabilities and market demands. AustCyber, an industry-led not-for-profit company, is part of the Australian Government's $250 million *Industry Growth Centres Initiative* and the *2016 Cyber Security Strategy*. It plays a key role in supporting the development of national cyber security capability by helping Australia's cyber security sector overcome challenges to innovation, productivity and growth.

There are particular sectors where Australia already has comparative advantages in cyber security capability, which are described in Australia's *Cyber Security Sector Competitiveness Plan*. To promote these sectors, Australia will proactively identify opportunities in key overseas markets, lead trade delegations to these key markets, and encourage the use of Landing Pads (*see below*).

Australia supports the responsible export of cyber security solutions. To help promote responsible export worldwide, Australia actively supports international export control regimes such as the *Wassenaar Arrangement*. To help foster cyber innovation and good cyber security practice, Australia has led the discussion with Wassenaar Participating States to ease export restrictions on cyber security technology for defensive purposes.

LANDING PADS

As part of the *National Innovation and Science Agenda*, Austrade has established five Landing Pads in Berlin, San Francisco, Shanghai, Singapore and Tel Aviv. Landing Pads provide market-ready Australian start-ups/scale-ups with access to some of the world's most renowned innovation and start-up ecosystems. Participating start-ups/scale-ups have a short-term operational base for up to 90 days, where they will benefit from Austrade's global network of contacts and tailored business development assistance. The Landing Pads are situated in leading co-working spaces in each location.

Austrade is conducting a pilot program focused on cyber security start-ups and scale-ups in the San Francisco Landing Pad from January to April 2018. This activity is designed to build on the success of the Australian cyber security mission to San Francisco Bay Area in February 2017.

ATTRACT FOREIGN DIRECT INVESTMENT TO AUSTRALIA'S CYBER SECURITY SECTOR

Producing world-class cyber security research is one of Australia's national science and research priorities, as set out in the *National Innovation and Science Agenda*. We will continue to promote Australia as a location of choice for global cyber security companies looking to establish a base in the Indo-Pacific, and as a leading centre for cyber education and research.

Australia has identified cyber security and related digital technologies as a target sector for attracting investment. As part of its strategy to promote, attract and facilitate productive foreign direct investment, the Australian Government will continue to work collaboratively with state and territory governments to provide qualified potential investors with information on the Australian business and regulatory environment, market intelligence and investment opportunities, and advice on government programs and approval processes.

Australia will work through AustCyber to showcase our cyber security industry capabilities through an Australian *Cyber Week*. Annual workshops will follow thereafter to agree priority areas of focus in line with annual updates to Australia's *Cyber Security Sector Competitiveness Plan*.

AUSTRALIA WILL:

2.08 Showcase Australia's cyber security capabilities to international customers and investors, including through delivery of an annual Australian Cyber Week

2.09 Promote and encourage cyber security start-ups through Landing Pads

2.10 Partner with the private sector to host a workshop to co-design how Australia promotes its cyber security industry internationally

CYBERCRIME

AUSTRALIA'S GOAL:

Stronger cybercrime prevention, prosecution and cooperation, with a particular focus on the Indo-Pacific

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- **Raise** cybercrime awareness in the Indo-Pacific
- **Assist** Indo-Pacific countries to strengthen their cybercrime legislation
- **Deliver** cybercrime law enforcement and prosecution capacity building in the Indo-Pacific
- **Enhance** diplomatic dialogue and international information sharing on cybercrime

Australia's economic prosperity and high adoption of technology mean we will remain an attractive target for cybercriminals in coming years. Cybercriminals are constantly adapting and evolving their techniques to exploit new technologies and defeat network defences. This tests the capacity of law enforcement agencies to adapt and respond. Australia will remain vigilant to the changing cybercrime threat environment in order to safeguard our economic interests.

As the volume and sophistication of cybercrime continues to grow, so too do its costs. It has been estimated that up to US$1.02 trillion in global economic growth will not be realised if we allow cybercrime to undermine public confidence in the digital domain. Addressing cybercrime in our region will create a safer commercial environment in which businesses can grow.

CYBERCRIME

Cybercrime is a low-risk, high-return criminal enterprise in which individuals and groups of actors leverage cyberspace for financial gain or other malicious ends. In Australia, the term cybercrime refers to crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It also includes crimes where computers facilitate an existing offence, such as online fraud or online child sex offences.

The vast majority of cybercrime targeting Australia originates overseas. Cybercrime is a global threat, but our region is particularly vulnerable. Countries in the region lose a third more business revenue to cybercrime than those in the European Union or North America.

Collectively, our region is only as resilient as our weakest link. Cybercriminals look to exploit the vulnerabilities of states in the early stages of developing the legislative and technical capabilities needed to fight cybercrime. These cybercrime safe havens are countries through or from which malicious cyber actors can conduct criminal operations with a very low risk of being identified, arrested, investigated, extradited or prosecuted.

In 2016, more than half of the world's netizens were found in the Indo-Pacific. But only 1.8 billion of the region's 4.1 billion people are yet online. This digital potential combined with the spread of ICT infrastructure and smart phone technology will produce a growing target audience for cybercriminals to exploit. It is in Australia's interest to help our neighbours improve their ability to prevent and respond to cybercrime. Doing so will underpin regional economic growth and create a safer environment in which Australian businesses can prosper.

Cybercriminals operate globally, so Australia will respond in kind. We will deepen bilateral, regional and global partnerships to increase cooperation and build our collective capacity to combat this threat. Cybercrime is a shared challenge and Australia encourages other countries to take an active role in initiatives that address this international issue.

Collaborative efforts to shut down safe havens complement Australia's ongoing national efforts to protect Australians from the harm of cybercriminals. The *2016 Cyber Security Strategy* committed the Government to enhance Australia's ability to respond to cyber security threats, including cybercrime. In 2017, the Government directed the Australian Signals Directorate (ASD) to use its offensive cyber capabilities to disrupt, degrade, deny and deter organised offshore cybercriminals. This capability is subject to stringent oversight, and consistent with domestic law and our obligations under international law. Strong cyber defences and law enforcement measures will continue to sit at the forefront of our response to cybercrime threats.

Australia embraces a comprehensive strategy of strong cyber defences, regional capacity building and national law enforcement efforts in its fight against cybercrime.

Raise cybercrime awareness in the Indo-Pacific

Individuals are at risk of falling victim to cybercrime if they don't understand online risks and the techniques used by cybercriminals. For this reason, public education, awareness and the development of basic cyber skills is a fundamental building block in the prevention of cybercrime, and an essential first step in undermining the success of cybercriminals in our region.

Increasing connectivity in the Indo-Pacific means that our region is home to a vast number of first-time Internet users. As these new users come online, it is important that they are equipped with the awareness needed to enjoy the benefits of the Internet safely. Cyber security education is necessary to inform people of good cyber security practices, such as avoiding the use of pirated software that cybercriminals can exploit to gain access to personal devices.

Australia is committed to improving cybercrime awareness levels in our region. *Cyber Safety Pasifika* (CSP) is a cyber safety and cybercrime education program led by the Australian Federal Police (AFP). CSP delivers cyber awareness to Pacific Island countries, including Tonga, Nauru, Cook Islands, Federated States of Micronesia, Marshall Islands, Papua New Guinea, Samoa, Solomon Islands and Vanuatu.

CSP provides cybercrime awareness materials and 'train-the-trainer' initiatives to ensure Pacific communities are equipped to identify cybercrime risks and engage safely online. Thanks to a 2017 program update, there are now 13 police officers from nine Pacific countries ready to train their colleagues and deliver up to date cybercrime education curriculums to schools and community groups across the region.

PRIVATE SECTOR ENGAGEMENT ON CYBERCRIME AWARENESS RAISING

The private sector has an important role to play in raising cybercrime awareness. Australian companies doing business around the region are well placed to contribute their good reputation, invaluable networks of contacts and contextual understanding to the effort. Australia will create public-private partnerships focused on improving regional awareness of cybercrime risks. This will not only be an important force multiplier but will also reinforce the message that cybercrime is a joint challenge that government and business must address together.

AUSTRALIA WILL:

3.01 Deliver cybercrime awareness training across the Indo-Pacific through public-private partnerships and the refreshed Cyber Safety Pasifika program

Assist Indo-Pacific countries to strengthen their cybercrime legislation

Raising public awareness will not prevent all cybercrime. Another effective way to respond to cybercrime is through a combination of stronger domestic legislative frameworks *within* countries and greater harmonisation of cybercrime legislation *between* countries.

Australia is committed to working with partners in the region to help strengthen their legal frameworks to address cybercrime. Robust cybercrime legal frameworks increase the risk of prosecution for would-be cybercriminals.

Strengthening cybercrime legislation raises the cost of 'business' for cybercriminals and is an important way of preventing cybercrime safe havens in our region.

Similarly, Australia advocates for the harmonisation of legal frameworks – that is, having similar conduct criminalised in all jurisdictions – to facilitate international cooperation on cybercrime. This ensures that criminals cannot evade justice by simply crossing borders.

THE BUDAPEST CONVENTION

Australia has been a party to the *Council of Europe Convention on Cybercrime* (the Budapest Convention) since 2013. It is a valuable mechanism to strengthen international cooperation on cybercrime, particularly through its provisions on mutual legal assistance. Countries are able to work together more effectively on trans-border investigations and prosecutions when domestic legal and law enforcement operational frameworks are harmonised in line with the provisions of the Budapest Convention. Reciprocal arrangements such as mutual legal assistance and intelligence sharing continue to be a critical mechanism for combatting cybercrime. Australia is keen to work with other countries to streamline these processes.

Australia works with countries in the region interested in acceding to the Budapest Convention by helping them achieve the required legislative reform. For example, substantial support from the Attorney-General's Department contributed to Tonga's recent accession to the Convention (*see Supporting Stronger Cyber Crime Legislation in Tonga, page 37*).

Australia will actively participate in the development of an Additional Protocol to the Budapest Convention on trans-border access to information. The Protocol will further articulate cooperation requirements between jurisdictions on providing access to electronic information, within appropriate conditions and safeguards. This will facilitate more effective mutual legal assistance through direct cooperation with service providers and between judicial authorities, joint investigation frameworks, and development of emergency assistance procedures. Australia is a member of the Drafting Group for the establishment of the Additional Protocol.

SUPPORTING STRONGER CYBERCRIME LEGISLATION IN TONGA

Australia worked closely with Tonga to strengthen its legislative capacity to respond to cybercrime threats and meet the obligations of the Budapest Convention by:

- facilitating a gap analysis of Tonga's legislation against the requirements of the Budapest Convention with an official from Tonga's Attorney General's Office (AGO) in 2014 through the Pacific Legal Policy Development Twinning Program;
- working with Tonga's AGO to draft a Computer Crimes Bill that ensured Tonga's legislation met its obligations under the Budapest Convention; and
- assisting Tonga's AGO with its consultations on the new Computer Crimes Bill prior to its introduction to Parliament during 2017.

Assisted by this collaboration, on 9 May 2017 Tonga became the first Pacific Island country to accede to the Budapest Convention. Tonga's experience and new legislative framework will provide a valuable model for other countries in the region.

PACIFIC ISLANDS LAW OFFICERS' NETWORK

Australia is also helping regional neighbours strengthen their cybercrime legislation by working with the Pacific Islands Law Officers' Network (PILON). PILON is a network of senior law officers from across the region that addresses law and justice issues common to Pacific countries. *PILON's Strategic Plan 2016–2018* recognises cybercrime as a priority legal issue. Through the network, Australia advocates for the broad adoption of the *Pacific Forensic Model Provisions*, which provide a consistent framework for the collection and use of electronic evidence. Australia will support future PILON activities in this area, building on its funding of the Pacific Cybercrime Workshop held in Tonga during May 2017 in partnership with PILON, the Tongan Government, and the Council of Europe.

This initiative is complemented by the 2017 expansion of *Cyber Safety Pasifika (CSP)*. The program now includes legislation and policy development activities, with Australia working in partnership with PILON and the Pacific Islands Chiefs of Police.

Australia will also support the Council of Europe's *Global Action on Cybercrime Extended* capacity building project (GLACY+) and *Cybercrime@Octopus* project that supports the adoption and implementation of the Budapest Convention in the Indo-Pacific.

AUSTRALIA WILL:

3.02 Promote the Budapest Convention as a best practice model for legislative responses to cybercrime and support accession to the Convention across the Indo-Pacific

3.03 Be active in the negotiation of an Additional Protocol to the Budapest Convention on trans-border access to information

3.04 Work with PILON to help strengthen cybercrime legislation in the region

Deliver cybercrime law enforcement and prosecution capacity building in the Indo-Pacific

Cybercrime legislation is not effective without the ability to enforce it. Australia is safer when countries in our region have the capacity to respond to cybercrime. Australia is committed to increasing the capacity of Indo-Pacific law enforcement agencies, prosecutors and judges.

The capacity of countries to investigate and prosecute cybercrime varies greatly in the Indo-Pacific. While some are leading in high-tech policing, others have only a nascent capability. Australia is working to close that gap.

Through its recently expanded *Cyber Safety Pasifika* (CSP) program, the AFP is actively partnering with law enforcement agencies in the region to enhance their capacity to address cybercrime. In partnership with the Federal Bureau of Investigation's (FBI) Legal Attaché Office in Canberra, the AFP coordinated a pilot three-day Cyber Investigations Skills Course for multiple Pacific Island countries in March 2017. The pilot, held in Brisbane, equipped 20 participating officers with basic cyber investigation skills including open source intelligence techniques. Through CSP, the AFP will continue to enhance the skills of Pacific police officers to manage cybercrime investigations.

The AFP also delivers cyber capacity building in the region through its support for the Jakarta Centre for Law Enforcement Cooperation (*see below*).

JAKARTA CENTRE FOR LAW ENFORCEMENT COOPERATION (JCLEC)

The JCLEC is a not-for-profit social enterprise in Semarang, Indonesia, jointly owned by the Indonesian National Police (INP) and the Australian Federal Police (AFP). The centre is supported by a broad range of public sector, civil society and private sector entities from across the world. The JCLEC supports global collaborative efforts to minimise the community harm caused by transnational crime and terrorism.

Since 2004, the JCLEC has facilitated 56 cybercrime capacity building activities for over 1,000 international participants. This has included courses on computer forensics, cybercrime and social media investigations, intelligence gathering and covert online engagement. Workshops delivered by the AFP at the centre have elevated INP's capacity to identify, extract and report on electronic evidence. This new digital forensic investigation capability means that direct operational exchanges can take place between INP and AFP leads.

In addition to skilled law enforcement, a country's prosecution and judiciary need to be equipped to address cybercrime cases effectively. Working together with multilateral partners such as the United Nations Office on Drugs and Crime (UNODC) and the Council of Europe, Australia will support the delivery of cybercrime training courses for prosecutors and judges in Indo-Pacific countries (*see Cybercrime Capacity Building with the United Nations Office on Drugs and Crime (UNODC)*).

In so doing, Australia will deliver a comprehensive cybercrime capacity building program to the region, tackling cybercrime from awareness, legislation, law enforcement, and prosecution perspectives.

CYBERCRIME CAPACITY BUILDING WITH THE UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)

Australia provided funding for UNODC cybercrime capacity building in Southeast Asia. The five-day training course was delivered in Bangkok during October 2016 to around 30 judges, prosecutors and investigators. The course was aimed towards ASEAN member countries, including Cambodia, Laos, Indonesia, Malaysia, Myanmar, the Philippines, Thailand and Vietnam. The training focused on cybercrime investigation and prosecution (including 'darknet' and hidden web services), hacking, device imaging, handling/using electronic evidence and online child sexual exploitation case investigation.

AUSTRALIA WILL:

3.05 Provide cybercrime training to law enforcement officers, prosecutors and judges across the Indo-Pacific

Enhance diplomatic dialogue and international information sharing on cybercrime

Australia is committed to collaborating with international partners to fight cybercrime collectively. Working together at the diplomatic and operational levels is critical to ensuring that cybercriminals have limited opportunities to exploit cyberspace for malicious purposes.

DIPLOMATIC DIALOGUE

High-level diplomatic engagement between Australia and its international partners on cybercrime helps generate common understanding and facilitate closer cooperation between counterparts. Cybercrime discussions are prioritised in Australia's diplomatic engagements.

Cybercrime was made a permanent agenda item for the *Australia-Indonesia Ministerial Council on Law and Security* in February 2017, and was a prominent agenda item at the first *Australia-China High Level Security Dialogue* in April 2017. Australia also engages actively on the issue in multilateral contexts such as the Pacific Islands Forum, ASEAN Regional Forum and East Asia Summit.

Australia and China 'will work together to counter malicious cyber actors, Internet distribution of child sex abuse material, e-mail scams and other transnational cybercrime activities, as well as to identify through consultation key incidents and carry out joint law enforcements'.

Joint Statement Australia-China High-Level Security Dialogue, Sydney 2017

PRIVATE SECTOR ENGAGEMENT IN INTERNATIONAL DIALOGUE ON CYBERCRIME

The international and multi-stakeholder nature of cyberspace necessitates broad engagement with global and private sector partners in the fight against cybercrime. The Ambassador for Cyber Affairs will lead delegations to participate in international public-private sector conversations, for example the 2017 INTERPOL World Conference in Singapore. These opportunities promote Australia's cyber security industry and its positive contribution to the global fight against cybercrime.

INFORMATION SHARING AND OPERATIONAL COLLABORATION

Australia complements its high-level diplomatic efforts with cybercrime threat information sharing and cooperation between international counterparts. This enables Australia and our partners to build a stronger threat picture of cybercriminal identities and methodologies, as well as share best practice mitigation.

Australia deploys individuals to partner countries around the globe to deepen information sharing links. The Australian Criminal Intelligence Commission (ACIC) has established two key working-level cyber partnerships. An ACIC Cybercrime Analyst is posted at the FBI International Cyber Crime Coordination Cell in the United States. Another is posted at the National Cybercrime Unit at the United Kingdom's National Crime Authority. These deployments enhance ACIC's ability to attribute real world identities to cybercriminals and develop strategic and operational intelligence products on cybercrime threats. Similarly, the AFP has established dedicated cybercrime liaison positions based in the United States and United Kingdom.

The Australian Transaction Reports and Analysis Centre (AUSTRAC) recently established a Cyber Operations team. This team focuses on the financial aspects of transnational cyber-enabled crime, tracking criminal financial transactions that occur online. The team harnesses established relationships with AUSTRAC partner agencies, FinTech partners and international networks, and develops new relationships with industry. AUSTRAC will continue to collaborate with partner Financial Intelligence Units (FIUs) and participate in international forums, including the Egmont Group of FIUs, to build its capacity to produce financial intelligence on virtual currencies and cybercrime.

Australia engages strongly with multilateral law enforcement information sharing networks such as INTERPOL and EUROPOL. The INTERPOL National Central Bureau Canberra, hosted by the AFP, is a conduit for the sharing of cybercrime information and intelligence with law enforcement agencies in the 190 INTERPOL member countries. The INTERPOL Global Complex for Innovation in Singapore also hosts an AFP Cybercrime Investigator in a leadership role.

EUROPOL, an intelligence focused support platform for law enforcement, hosts the European Cyber Crime Centre in The Hague in the Netherlands. Australia seconds an AFP Investigator to the centre, which targets technology-enabled serious crime and cyber disruption. The AFP also has a dedicated Cybercrime Liaison Officer based within the EUROPOL Joint Cybercrime Action Task Force. These secondees provide expert support to international efforts, as well as sourcing cybercrime threat information for Australian agencies on a regular basis.

Australia also participates in practical cybercrime cooperation mechanisms such as the International Cyber Crime Operations Summit (ICCOS). This initiative aims to degrade high-level cybercrime capabilities through information sharing and operational collaboration. The ICCOS membership

includes Australia, the United States, United Kingdom, Canada, New Zealand, Germany, Netherlands, France and EUROPOL. The collaborative group was responsible for the takedown of the Avalanche cybercriminal infrastructure in December 2016, judged to be the largest and most successful international operation of its kind to date.

The Five Eyes Law Enforcement Group Cyber Crime Working Group, held in conjunction with the ICCOS, is another framework through which Australia cooperates on cybercrime. Through the group, the United States, United Kingdom, Canada, New Zealand and Australia share operating pictures and best practice approaches, maximise resources and act as an operational force multiplier in the fight against cybercrime.

AUSTRALIA WILL:

3.06 Seek further opportunities to participate in strategic-level engagement on combatting transnational cybercrime

3.07 Share cybercrime threat information and enhance operational collaboration with international partners to fight transnational cybercrime

INTERNATIONAL SECURITY & CYBERSPACE

AUSTRALIA'S GOAL:

A stable and peaceful online environment

TO ACHIEVE THIS GOAL AUSTRALIA WILL:

- **Set** clear expectations for state behaviour in cyberspace
- **Implement** practical confidence building measures to prevent conflict
- **Deter and respond** to unacceptable behaviour in cyberspace

The history of international security and warfare reflects the history of technological innovation. Today, cyberspace is an increasingly important area for cooperation and competition between states. As the strategic significance of cyberspace increases, more groups will try to exert power through it. Likewise, as dependence on global ICT networks increases, the potential costs of disruption are large, and growing.

Malicious activity in cyberspace has the potential to threaten international peace, security and stability. A large scale cyber attack on critical infrastructure would have severe implications for international security. However, international peace, security and stability could be equally threatened by the cumulative effect of repeated low-level malicious online behaviour. It is the scale and effect of the activity, not necessarily the actor, means or method that determine its malicious nature.

Australia is committed to a peaceful and stable cyberspace. We recognise that, as more and more states seek to exert power through cyberspace, there is increased potential for activities in this domain to lead to misperception, miscalculation, escalation and, in the most extreme cases, conflict between states. Australia will be stronger when we manage these risks in cooperation with international partners.

Australia seeks a more mature and transparent conversation about what states are doing in cyberspace. In the face of clear evidence to the contrary, it is no longer plausible to simply deny that states are active in cyberspace. Recognition that states have legitimate rights to develop and use cyber capabilities must go hand in hand with recognition that states are obliged to ensure their use of cyber capabilities accords with international law and norms of acceptable behaviour.

Acknowledgement that states are developing cyber capabilities does not contradict Australia's commitment to maintaining a peaceful and stable online environment. Rather, acknowledging the existence of these capabilities fosters the understanding that, just like in the physical domains, states' activities in cyberspace do not occur in a vacuum. States have rights, but they also have obligations.

Good progress has been made in delineating the boundaries of what is and isn't acceptable behaviour by states in cyberspace. But some states are testing, and even crossing, those boundaries. It is important that there are consequences for those who act contrary to this consensus.

The 2016 Presidential Election in the United States focused the world's attention on the potential for cyber-enabled information operations to interfere with processes underpinning democracy. Such actions have particular implications for connected, open and democratic societies like Australia. This behaviour is unacceptable. We will guard against attempts to use such measures to interfere in Australia's domestic affairs or undermine our institutions. More broadly, Australia will cooperate with international partners to deter and respond to malicious cyber activity that endangers international peace, security and stability.

In parallel to Australia's engagement in international security and cyberspace, the Government is enhancing cooperation with international partners to detect and limit terrorist and other misuse of the Internet as a tool to recruit and radicalise. International efforts in this regard are led by Australia's Ambassador for Counter-Terrorism in close cooperation with the Attorney-General's Department's Countering Violent Extremism Centre.

Set clear expectations for state behaviour in cyberspace

International law has developed over centuries. It comprises rules and principles that, inter alia, govern relations between states. While the domain may be comparatively new, the rules are not. International law applies in cyberspace.

The unique attributes of cyberspace mean that existing international law can be usefully complemented by agreed norms of behaviour. Alongside states' international legal obligations, these non-binding norms establish clear expectations of proper state behaviour in cyberspace.

INTERNATIONAL LAW APPLIES TO CYBERSPACE

As observed above, international law applies to states' conduct in cyberspace just as it applies to states' conduct in the physical domains. The existing international legal framework helps reduce the risk of conflict by articulating clear obligations for how states interact.

In some instances, it is useful to clarify how particular rules, principles and bodies of international law apply to states' conduct in cyberspace. Much of the hard work is already done, but this continues to be a work in progress – particularly as digital technologies continue to evolve at a rapid pace.

CYBER ATTACK

The Australian Government defines cyber attack as a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity.

This definition was developed in 2011 after extensive policy and legal consultation. It was subsequently used to affirm that the provisions of the ANZUS Treaty allow Australia and the United States to consult each other in the event of a cyber attack on either party.

Australia reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the availability of the doctrine of countermeasures in response to internationally wrongful acts.

The cumulative reports of the *UN Group of Governmental Experts on Developments in the Field of Information and Communication Technologies in the Context of International Security* (UN Group of Governmental Experts) have contributed to our collective understanding of how international law applies to states' conduct in cyberspace. The Tallinn Manuals are also an important academic contribution to international legal dialogue in this area.

Australia encourages states to continue to exchange views on how particular rules and principles of international law apply to state conduct in cyberspace. This will facilitate the development of deeper understandings and expectations – not just among states, but also within the private sector, civil society and academia.

AUSTRALIA WILL:

4.01 Periodically publish Australia's position on the application of relevant international law to state conduct in cyberspace (the first such publication is at Annex A)

INTERNATIONAL SECURITY AND THE PRIVATE SECTOR

The stability of cyberspace benefits the private sector and governments, and our interests in maintaining a peaceful online environment are complementary. A significant proportion of the world's Internet infrastructure is owned and operated by the private sector. This means the private sector is well placed to contribute to discussions on the practicality of norms, and champion their implementation.

SUPPORT ROBUST NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

Norms establish clear expectations of behaviour in specific circumstances by specific groups. By signalling acceptable behaviour of states in cyberspace, norms promote predictability, stability and security. Norms must be developed consistent with international law.

Shared understandings of responsible behaviour also provide the basis for the international community to respond when these shared expectations are not met. Understanding of and adherence to norms by states increases the predictability of state actions, thereby reducing the risk of misunderstandings that could lead to conflict.

The 2015 Report of the *UN Group of Governmental Experts* set out 11 such norms (*see Annex B*). Also in 2015, G20 leaders agreed that 'no country should conduct or support ICT-enabled theft of intellectual property, including state secrets or other confidential business information, with the intent of providing competitive advantages to companies or the commercial sector.'

Australia affirms its commitment to act in accordance with these norms.

> Australia and China 'agreed to support the work of the UN Group of Governmental Experts and to act in accordance with its reports…Australia and China agreed not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of obtaining competitive advantage.'
>
> *Joint Statement Australia-China High-Level Security Dialogue, Sydney, 2017*

Australia engages in multi-agency cyber policy and cyber security dialogues with countries including Canada, China, India, Indonesia, Japan, New Zealand, the Republic of Korea, the United Kingdom and the United States. These dialogues are an opportunity to deepen understanding of responsible state behaviour in cyberspace and foster cooperation to deter and respond to malicious cyber activities.

AUSTRALIA WILL:

4.02 Facilitate advanced policy development and promote informed public discussion on acceptable state behaviour in cyberspace through engagement with academics and experts in this field

4.03 Seek high-level reaffirmations from states that they will act in accordance with international law and identified norms of responsible state behaviour in cyberspace

4.04 Partner with countries in the Indo-Pacific to advance our combined understanding of how international law and norms of responsible state behaviour apply in cyberspace through bilateral engagement and regional and multilateral forums

Implement practical confidence building measures to prevent conflict

Australia is committed to taking practical action to support international peace and security. Confidence building measures foster trust between states to prevent misunderstandings that could lead to conflict. They include transparency measures, risk reduction measures and cooperative measures. Confidence building measures are one of the most important tools in our diplomatic toolkit. Australia is committed to implementing these measures to maintain a peaceful and stable online environment.

Australia will look for opportunities for practical cooperation on cyber issues with ASEAN partners. Working together to harness the opportunities and address the shared challenges of cyberspace will be a key theme of the Australia-ASEAN Special Summit in March 2018.

RISK REDUCTION MEASURES

Risk reduction measures build confidence in states' capacity to collaborate to respond to specific instances of malicious cyber activity without escalation to conflict.

An example of a risk reduction measure could be the development of a database of regional policy and diplomatic points of contact for use in the event of a cyber incident. Knowing who to call in times of tension reduces the risk of miscommunication and, in turn, this reduces the risk of escalation to conflict. The very act of compiling the directory of contacts can be a confidence building measure in and of itself.

A lot of good work has already been done in this field. A number of different bodies have identified practical confidence building measures that increase stability and reduce risk, including the UN Group of Governmental Experts, the ASEAN Regional Forum, the Organization for Security Cooperation in Europe and the Organization of American States.

The task now is to move from identifying risk reduction measures to operationalising them. In doing so, Australia will prioritise measures which have the greatest impact on reducing risk to international peace and security. Our focus will be on putting in place measures that enable states to cooperate in situations of tension or crisis.

AUSTRALIA WILL:

4.05 Develop a framework to exchange policy and diplomatic contacts, including bilaterally, to facilitate communication in times of crisis or tension arising from significant cyber incidents that have the potential to threaten international peace, security and stability

4.06 Work with regional organisations to conduct risk reduction workshops to enhance our capacity to manage and respond to cyber incidents that threaten international peace, security and stability, including exercising national and regional responses to severe cyber incidents

TRANSPARENCY MEASURES

Transparency measures provide insight into states' activities. They reduce the risk of miscommunication as well as the likelihood of overreaction.

Australia's *2016 Cyber Security Strategy*, the *2016 Defence White Paper*, the forthcoming *Foreign Policy White Paper* and this Strategy are all examples of transparency measures. Other examples include cyber policy dialogues, sharing Australia's national cyber governance structures (including cyber incident management arrangements), and outlining Australia's position on how international law applies to state conduct in cyberspace.

Another area where Australia encourages greater candidness is in relation to the military use of offensive cyber capabilities. Just as more and more states are embracing the opportunities of cyberspace to improve service delivery and drive economic growth, it is unsurprising that more and more states are exploring military applications of cyberspace. In and of itself this is not a concern – provided that states acknowledge that military activities in cyberspace are governed by the same sets of rules as military activities in the physical domains. These rules, developed over centuries, restrict and regulate unacceptable conduct.

Australia recognises that, just like other military capabilities, some details of cyber capabilities and operations will need to remain classified. By way of analogy, Australia is transparent about the rules that govern the use of conventional capabilities such as missiles on our warships; however, we do not discuss the specifics of the capability, nor would we reveal details of particular operations. We will take the same approach to discussing cyber capabilities. Acknowledgement of these capabilities does not contradict our commitment to a stable and peaceful online environment. Instead it fosters the understanding that states' activities in cyberspace have limitations and obligations, just as they do in the physical domains (*see Conduct and Authorisation of Offensive Cyber Capability in Support of Military Operations, page 55*).

COOPERATIVE MEASURES

Cooperative measures promote collaboration between states based on a mutual commitment to improve cyber resilience and reinforce a peaceful and stable online environment.

Cooperative measures could include exchanging information on best practices in responding to cyber incidents or capacity building programs like Australia's new *Cyber Cooperation Program* (*see the Comprehensive & Coordinated Cyber Affairs chapter*).

Australia's *Cyber Cooperation Program* facilitates the development of comprehensive, forward-leaning policies, legislative frameworks and cyber governance institutions to empower regional partners to safely embrace the benefits of connectivity. It will also provide opportunities for Australia to learn and adopt emerging best practices to strengthen our own cyber policy and security measures.

Development of robust cyber policy and well-resourced cyber governance institutions will mean that the collective capacity of states to respond to cyber incidents is enhanced, messaging to potential adversaries is consistent and security is strengthened overall. It will also empower Indo-Pacific states to participate in international discussions about the future of cyberspace in an inclusive manner.

AUSTRALIA WILL:

4.07 Hold cyber policy dialogues to discuss and work with partners to achieve priority goals on international cyber issues, including international law, norms of responsible state behaviour and confidence building measures

4.08 Foster recognition through diplomatic outreach and defence engagement that military offensive cyber capabilities are subject to the same limitations and obligations as any other military capability

Deter and respond to unacceptable behaviour in cyberspace

The international community has made good progress delineating the boundaries of what is and isn't acceptable behaviour in cyberspace – but some states are testing those boundaries. Like many others, Australia is concerned by the increased willingness of states and non-state actors to pursue their objectives by undertaking malicious cyber activities contrary to international law and identified norms of responsible state behaviour.

Having established a firm foundation of international law and norms, the international community must now ensure there are effective consequences for those who act contrary to this consensus. Australia is committed to countering, deterring and discouraging malicious cyber activity, especially by states and their proxies. We will work with partners to strengthen global responses to unacceptable behaviour in cyberspace.

An architecture for cooperation amongst states is needed. This includes mechanisms to respond to unacceptable behaviour in cyberspace in a timely and agile manner, within the existing framework of international law. Achieving this cooperation requires creative thinking to build a flexible range of existing and novel response tools, and a nimble coordination mechanism to implement them effectively.

Australia's responses to malicious cyber activity could comprise law enforcement or diplomatic, economic or military measures as appropriate for the circumstances. This could include, but is not restricted to, offensive cyber capabilities that disrupt, deny or degrade the computers or computer networks of adversaries. Regardless of the context, Australia's response would be proportionate to the circumstances of the incident, would comply with domestic law, and be consistent with our support for the rules-based international order and our obligations under international law.

Attribution of malicious activity is necessary to enable a range of response options. Depending on the seriousness and nature of an incident, Australia has the capability to attribute malicious cyber activity in a timely manner to several levels of granularity – ranging from the broad category of adversary through to specific states and individuals.

Australia's strong cyber security posture underpins our ability to deter and respond to serious incidents and unacceptable behaviour in cyberspace. It ensures that Australia can discourage, detect, respond to, and contain malicious cyber activity.

CONDUCT AND AUTHORISATION OF OFFENSIVE CYBER CAPABILITY IN SUPPORT OF MILITARY OPERATIONS

Australian offensive cyber capabilities are held by the Australian Signals Directorate (ASD). Australian offensive cyber operations are conducted by ASD personnel. Offensive cyber operations in support of Australian Defence Force (ADF) operations are planned and executed by ASD and Joint Operations Command under direction of the Chief of Joint Operations. All operations are conducted in accordance with international law and domestic law, including the *Commonwealth Criminal Code Act 1995* and the *Intelligence Services Act 2001*.

Like any other military capability, use of this offensive cyber capability in support of military operations is governed by ADF Rules of Engagement (ROE). ROE are informed by and consistent with domestic and international law, including the Law of Armed Conflict (International Humanitarian Law). Offensive cyber capabilities are also subject to ASD's existing legislative and oversight framework, including independent oversight by the Inspector-General of Intelligence and Security.

The *2016 Cyber Security Strategy* and the *2016 Defence White Paper* boosted Australia's cyber security capabilities. Australia is strengthening the Australian Cyber Security Centre, establishing a multi-layered national cyber threat sharing network. The Australian Defence Force's (ADF) Information Warfare Division will shape the development of ADF cyberspace capabilities to secure and protect ADF networks and systems, and support the integration of cyber capabilities into ADF operations.

Australia has also established the Critical Infrastructure Centre to work cooperatively with owners and operators to manage the complex and evolving national security risks from foreign involvement in Australia's critical infrastructure. The centre develops risk assessments to support Government decision-making on foreign investment in assets that may affect national security. Australia's overall goal is to harden our networks, deter unacceptable behaviour in cyberspace, and promote an open, free and secure online environment.

AUSTRALIA WILL:

4.09 Review Australia's range of options to deter and respond to unacceptable behaviour in cyberspace, especially those involving state actors and their proxies

4.10 Undertake diplomatic action to support an international cooperative architecture that promotes stability, and responds to and deters unacceptable behaviour in cyberspace

INTERNET GOVERNANCE & COOPERATION

AUSTRALIA'S GOAL:

An open, free and secure Internet, achieved through a multi-stakeholder approach to Internet governance and cooperation

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- **Advocate** for a multi-stakeholder approach to Internet governance that is inclusive, consensus-based, transparent and accountable
- **Oppose** efforts to bring the management of the Internet under government control
- **Raise** awareness across the Indo-Pacific of Internet governance issues and encourage engagement of regional partners in Internet governance and cooperation discussions

The Internet is a network of networks. A suite of technical protocols and an array of communications technologies give the Internet its form. This ecosystem of technologies, on which the Internet depends, has evolved over time to maintain and improve the security, stability and resilience of the Internet. The governance of this ecosystem is an international issue, with implications for us all. Multi-stakeholder Internet governance underpins the open, free and secure nature of the Internet, on which our economies and societies rely.

OPEN, FREE AND SECURE CYBERSPACE

An **open** cyberspace is interoperable across borders and accessible to all; it facilitates unrestricted participation and the free flow of information, driving inclusive online collaboration, innovation and growth.

A **free** cyberspace means people are not burdened by undue restrictions on their access to and use of cyberspace; and their human rights are protected online as they are offline so that cyberspace remains a vibrant force for economic, social and cultural development.

A **secure** cyberspace is safe, reliable and resilient; it fosters an environment of trust so that individuals, businesses and governments can engage online with confidence and realise the opportunities and minimise the risks of the digital age.

Reflecting its collaborative development, governance of the Internet is shaped by a multi-stakeholder approach. This approach allows the private sector, academia, technical experts, civil society and governments to contribute equally to discussions on the policy and technical management of the Internet. The multi-stakeholder approach is a proven model for responding to complex policy and technical challenges associated with the development of the Internet. These policy challenges include security concerns, consumer protection, maintaining legitimate competition and the management of cross-border data flows.

However, the multi-stakeholder model of Internet governance cannot be taken for granted. As the strategic importance of cyberspace increases, so too will strategic competition over its future development.

MULTI-STAKEHOLDER APPROACH TO INTERNET GOVERNANCE

The multi-stakeholder approach to Internet governance is a decentralised governance model that places individuals, industry, non-commercial interests and government on an equal level. The multi-stakeholder approach allows for community-based policy-making.

Advocate for a multi-stakeholder approach to Internet governance

Australia is a strong supporter of an open, free and secure Internet, and advocates for policy settings that support this position. The multi-stakeholder approach recognises that all stakeholders have a valuable contribution to make. Importantly, and by its very design, the multi-stakeholder approach prevents any group (including governments) from exerting undue influence over the future of the Internet. The multi-stakeholder approach offers a set of tools and practices that allow diverse stakeholders to participate alongside each other, share ideas, and develop consensus-based policy in the interest of all users of the Internet.

Multi-stakeholder consultations and discussions on the Internet's technical and policy frameworks are conducted at international, regional and national levels through Internet governance forums. Australia will continue to ensure that its contributions in these forums are centred on well-reasoned policy positions. We will also continue to work in close coordination with the private sector, academia, technical experts and civil society.

Australia is committed to negotiating in good faith to reach consensus with other countries and non-government stakeholders about the Internet's policy settings.

KEY INTERNATIONAL FORUMS

Australia will continue its engagement in key international multi-stakeholder organisations and forums. This includes the Internet Corporation for Assigned Names and Numbers (ICANN) and global and regional Internet Governance Forums (IGFs). ICANN is responsible for coordinating the global domain name system and is the major decision-making forum within the current Internet governance framework. The global IGF provides a platform for discussion of Internet-related public policy issues and idea sharing around maximising opportunities and minimising challenges associated with the Internet.

STRENGTHEN AUSTRALIA'S DOMESTIC MULTI-STAKEHOLDER COOPERATION

Australia is committed to strengthening domestic multi-stakeholder mechanisms for Internet governance and cooperation. We are committed to consulting with a wide range of both government and non-government stakeholders domestically, regionally and internationally to develop public policy positions across the full spectrum of cyber affairs.

Consultation with the local Internet community has identified a need for more opportunities for multi-stakeholder discussion in Australia on cyber policy issues, in particular Internet governance and cooperation.

Australia will support annual community-led Internet governance dialogues run by a voluntary steering committee with focused and topical agendas. These dialogues will include government and non-government stakeholders including consumer groups, technical experts, private sector stakeholders (such as registries and hosting providers) and, critically, users of the Internet.

Better multi-stakeholder cooperation in Australia will help inform the positions of all Internet stakeholders, including the Government. This will contribute to coordinated Internet governance efforts domestically and internationally.

PRIVATE SECTOR ENGAGEMENT

Australia will continue to work closely with private sector partners to ensure their voice is represented in international discussions on the future of the Internet. Most of the infrastructure on which the Internet runs is owned or managed by the private sector. The private sector has also largely driven the innovation at the heart of the Internet's success. Therefore, including the perspective of the private sector is critical to the longer term growth and sustainability of the digital ecosystem.

NET NEUTRALITY

Australia is a strong advocate of an open and competitive Internet. Internationally, there has been a focus on telecommunications companies gaining commercial advantage by giving priority to certain types of data, or data from certain sources, rather than applying the principle of 'net neutrality', that is: treating all data equally.

Concerns about net neutrality have not been as prominent in Australia as in other countries because our market structure fosters strong retail competition and provides significant consumer choice. This allows consumers who are dissatisfied with their provider to take their business elsewhere. In the absence of a demonstrated problem, Australia has taken the view that regulation on net neutrality is unnecessary. Our telecommunications regulations, in addition to our general competition law – the *Competition and Consumer Act 2010* – provide mechanisms to address competition concerns.

Australia supports measures that deal with anti-competitive conduct in the supply of services on the Internet. Anti-competitive conduct on the Internet includes blocking websites, intentionally slowing bandwidth speeds (bandwidth throttling) and, in some circumstances, data prioritisation. These practices can disadvantage certain businesses, such as over the top service providers and content providers.

However, care needs to be taken to ensure that legitimate competitive conduct and traffic management practices aren't prevented. Transparency around traffic management practices can help assure customers in this regard.

AUSTRALIA WILL:

5.01 Advocate for an open, free and secure Internet, underpinned by a multi-stakeholder approach to Internet governance and cooperation

5.02 Support an annual community-led Australian Internet governance and cooperation forum

5.03 Outline Australia's strong commitment to fostering fair and effective competition online, emphasising a preference for general competition law

Oppose efforts to bring the management of the Internet under government control

Australia recognises that there is an appropriate role for governments to play in Internet governance, but it is not one of control. Some states pursue a state-centred model of Internet governance in response to new public policy challenges raised by the advent of the Internet.

A state-centred model of Internet governance would restrict and fragment the network, inhibit innovation and constrain the enormous potential of the Internet. States should resist policy responses that put at risk an open, free and secure cyberspace.

Australia opposes moves to bring governance and technical management of the Internet under the control of governments or into the United Nations (UN) system, for example within the UN International Telecommunications Union. Instead, Australia advocates for the improvement of existing mechanisms of multi-stakeholder governance. This approach will ensure that governance of the Internet remains inclusive, consensus-based, transparent and accountable.

This will be particularly important as the Internet continues to evolve and support a range of emerging technologies. Governance of the Internet of Things, rules for the use of data, and privacy and trust online are all issues demanding a collaborative approach to Internet governance.

AUSTRALIA WILL:

5.04 Oppose efforts to bring the management of the Internet under government control

Raise awareness of Internet governance issues across the Indo-Pacific

Australia is working to foster closer engagement with our neighbours in the Indo-Pacific on Internet governance issues so that we can work together to shape the Internet of the future.

Australia will provide practical support for Indo-Pacific countries to engage in international Internet governance and cooperation discourse. Australia will continue to build relationships with regional Internet governance stakeholders and coordinate our policy positions with others in the region.

Australia will also support regional Internet governance forums, workshops and events. We will explore opportunities to collaborate with private sector stakeholders to achieve greater awareness of, and interest in, Internet governance issues across the region. Internationally, Australia seeks to raise awareness among international stakeholders about the unique Internet governance and cooperation challenges faced by Indo-Pacific countries.

AUSTRALIA WILL:

5.05 Build the capacity of Indo-Pacific partners to engage in regional and international discussion on Internet governance and cooperation

HUMAN RIGHTS & DEMOCRACY ONLINE

AUSTRALIA'S GOAL:

Human rights apply online as they do offline

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- **Advocate** for the protection of human rights and democratic principles online
- **Support** international efforts to promote and protect human rights online
- **Ensure** respect for and protection of human rights and democratic principles online are considered in all Australian aid projects with digital technology components

Cyberspace has provided an unparalleled opportunity for democratic participation around the world, as well as the global promotion, protection and fulfilment of human rights.

Democratic debate on policy and ideas takes place online just as it does offline. The Internet has empowered individuals across the globe to have their voices heard and has equipped governments to better respond to citizens' needs. Australia encourages states to make full use of online tools to strengthen democratic processes.

However, the decentralised and largely unregulated nature of online conversations leaves democratic processes vulnerable to malicious interference. Cyber-enabled influence operations during elections can undermine democratic processes. This has the potential to fundamentally distort political debate and democratic outcomes.

Human rights apply online just as they do offline. The Internet provides important platforms for freedom of expression and freedom of association. Instantaneous communication via the Internet helps raise awareness of human rights entitlements and human rights abuses. Stories and images of human rights abuses can be shared instantly across the world, inflicting significant reputational damage on perpetrators. This assists government authorities, non-government organisations and other stakeholders to hold human rights violators to account.

Some countries deny human rights online. In some countries, people are increasingly subject to undue restrictions on and contraventions of their rights. Illicit monitoring and targeted hacking, the arrest and intimidation of online activists, content censorship and Internet shutdowns are just some of the approaches taken to restrict human rights online. These measures are regularly employed under the pretext of national security, but are often vehicles for states to maintain political control and economic advantage.

Advocate for the protection of human rights and democratic principles online

An open, free and secure cyberspace allows human rights and democratic principles to be exercised online. Australia's commitment to human rights underpins our engagement with the international community.

Australia is a committed supporter of human rights and democracy, both online and offline. Australia believes that the universal protection and promotion of human rights and democratic principles online is vital to achieve lasting peace, security, freedom and dignity for all.

Of particular relevance in cyberspace are the right to freedom of expression, the right to freedom of association, and the protection against arbitrary interference with privacy. Each of these rights are enshrined in the *International Covenant on Civil and Political Rights*.

Australia is committed to seeing freedom of expression protected online, just as it is offline. Australia condemns politically motivated Internet censorship, Internet shutdowns, illicit monitoring, targeted hacking, and the arrest and intimidation of online activists, journalists and others.

KEY INTERNATIONAL FORUMS

Australia's support for human rights online has been articulated through a number of United Nations (UN) Human Rights Council and UN General Assembly resolutions and statements, and by virtue of its membership of the Freedom Online Coalition. Australia is seeking a seat on the Human Rights Council for the 2018–2020 term, and the right to freedom of expression is a key element of our campaign pledges. This reflects Australia's commitment to ongoing promotion and protection of human rights, both online and offline.

An open, free and secure cyberspace also strengthens social, cultural and political rights by facilitating greater connectivity and engagement within and between populations. Attempts to circumscribe and restrict use of the Internet impinges on these rights. Australia will use bilateral and international engagement to raise concerns about impermissible restrictions on human rights online. We will also raise concerns about cyber-enabled interference in democratic processes.

Australia will couple advocacy with capacity building programs in the Indo-Pacific, which will raise awareness among regional governments of human rights obligations online and offline. Also important is equipping law enforcement agencies with the capacity to detect human rights abuses online, disrupt these abuses and safeguard against future abuses. Australia will also encourage and support partner countries to engage in international forums that work to protect human rights online.

PRIVATE SECTOR ENGAGEMENT

Australia will demonstrate our commitment to the United Nations (UN) *Guiding Principles on Business and Human Rights*. Australia consults regularly with the private sector on human rights and has established a multi-stakeholder advisory group on businesses and human rights. Australia will use these mechanisms to discuss human rights and democracy online.

AUSTRALIA WILL:

6.01 Advocate to uphold and protect human rights and democratic freedoms online

6.02 Share concerns about, and aim to prevent, undue restrictions of human rights online as well as cyber-enabled interference in democratic processes

6.03 Fund capacity building in the Indo-Pacific to raise awareness of states' human rights obligations online

Support international efforts to promote and protect human rights online

Non-government organisations play a vital role in the protection of human rights and democratic freedoms online. These organisations often have broad civil society networks and are acutely aware of the challenges facing human rights defenders in the digital environment.

In addition to its international human rights advocacy efforts, Australia will provide financial support to international organisations protecting human rights and democratic freedoms online, such as the Freedom Online Coalition and Digital Defenders Partnership (*see below*).

FREEDOM ONLINE COALITION AND DIGITAL DEFENDERS PARTNERSHIP

The Freedom Online Coalition is a group of 30 member governments, including Australia, which work together to support Internet freedom and protect human rights online. The Freedom Online Coalition's founding declaration commits to the principle that the human rights people have offline, enjoy the same protection online.

Coalition members share information on violations of human rights online and coordinate diplomatic efforts to eliminate measures that curtail human rights online. The Coalition also provides a platform for multi-stakeholder engagement on human rights online, including with the private sector.

In support of this effort, the Digital Defenders Partnership, which emerged from the Freedom Online Conference in Kenya in 2012, provides grants that support defenders of human rights online, including non-government organisations, civil society, journalists and media organisations.

AUSTRALIA WILL:

6.04 Support non-government organisations that defend human rights online

Ensure respect for and protection of human rights and democratic principles online

Increased connectivity and access to the Internet can bring many benefits. However, increased connectivity also increases the possibility for misuse of the Internet to restrict human rights and opportunities for democratic participation.

To guard against this, Australia will ensure respect for and protection of human rights online is included in Australian development assistance programs that include digital technology components. Australia will encourage governments and non-government organisations to ensure that technology and cyberspace are used in accordance with human rights obligations.

AUSTRALIA WILL:

6.05 Provide guidance to ensure that human rights online are protected in Australian aid and non-government projects with digital technology components

TECHNOLOGY FOR DEVELOPMENT

AUSTRALIA'S GOAL:

Digital technologies are used to achieve sustainable development and inclusive economic growth in the Indo-Pacific

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- **Improve** connectivity and access to the Internet across the Indo-Pacific, in collaboration with international organisations, regional governments and the private sector
- **Encourage** the use of resilient development-enabling technologies for e-governance and the digital delivery of services
- **Support** entrepreneurship, digital skills and integration into the global marketplace

Digital technologies are profound enablers of sustainable development and inclusive economic growth. The spread of the Internet and digital technologies has facilitated greater connectivity, reducing physical and functional barriers between people, businesses and governments.

The United Nations (UN) *2030 Agenda for Sustainable Development* recognises digital technologies as vital to ending poverty, expanding access to quality education, achieving gender equality and social inclusion, promoting inclusive economic growth, improving health outcomes and supporting cross-sectoral innovation.

Connectivity varies greatly across the world, meaning that the socio-economic opportunities of the digital age are not evenly experienced. The Indo-Pacific is highly diverse, comprising of developed, emerging and least developed economies, each at a different point in their digital journey.

The Indo-Pacific is home to countries with some of the highest, and fastest growing, connectivity rates. In many ways, the Indo-Pacific is at the forefront of the world's digital revolution. Many Indo-Pacific countries are global leaders in digital economics, cyber security, the production and global exportation of new technologies, and other cyber-related areas. The region is already the largest contributor to the world's digital markets and, by 2020, will contribute $1.4 trillion to global e-commerce. However, the Indo-Pacific is also home to some of the world's least connected countries, where Internet penetration still sits in single digits and digital opportunities are yet to be fully harnessed. Digitally enabled development must take into account inter-regional differences in connectivity and digital readiness.

Digital divides across the Indo-Pacific are the product of several factors. In some countries, insufficient financial resources and challenging topography complicate the establishment of essential communication infrastructure. In others, low literacy rates, limited technical skills, socio-cultural constraints, unaffordable service costs or unreliable electricity supply undermine access to, and use of, digital technologies. Access limitations are particularly stark for women and girls, older persons, people with disabilities, indigenous, ethnic and religious minorities, rural populations and the poor.

Australia is committed to working bilaterally, regionally and multilaterally to bridge digital divides across the Indo-Pacific. Australia is also committed to encouraging innovative uses of digital technologies to support sustainable and inclusive development.

'Information Communication Technologies can be an engine for achieving the Sustainable Development Goals. They can power this global undertaking.'

United Nations Secretary-General Ban Ki-moon, December 2015

Improve connectivity and access to the Internet across the Indo-Pacific

Internet access is a prerequisite for the effective operation of most digital technologies. Connectivity is therefore a fundamental requirement for technology-enabled development. Australia will contribute to international efforts to improve connectivity and Internet access across the Indo-Pacific. This is a task of enormous social and economic importance: estimates suggest that for every 10 per cent increase in broadband Internet penetration, a country could increase its Gross Domestic Product growth by 1.4 per cent.

To facilitate increased connectivity, countries must have the necessary infrastructure. This includes submarine cables, satellites, cross-border fibre connections, cellular data services, Internet Exchange Points, and other emerging infrastructure technologies. Connectivity also fundamentally relies upon the availability, affordability and reliability of electricity supply.

Australian support for digital communications infrastructure in the Indo-Pacific is bringing connectivity to hundreds of thousands of people in some of the most remote places on earth. Australia contributed technical expertise and financial resources (in partnership with the World Bank and the Asian Development Bank) to lay a fibre-optic submarine cable connecting Samoa and Fiji. This has facilitated improved Internet access at more affordable prices. Australia has also supported projects to enhance mobile coverage in the Solomon Islands and Kiribati. In 2017–18, Australia will support the laying of a new submarine cable that will provide faster and more stable Internet connectivity to the Republic of Palau.

PRIVATE SECTOR ENGAGEMENT

The challenge of building adequate legal, regulatory and institutional frameworks across the Indo-Pacific will require collaboration with private sector stakeholders including telecommunications service providers and partners in the financial sector.

To make use of this base infrastructure, Internet services and Internet-enabled devices must be affordable and operate at sufficient speeds. Telecommunications market monopolies and high input costs present a significant barrier to ubiquitous Internet access. In order to improve affordability of access, it is essential to have in place the appropriate regulatory, legal and institutional frameworks. These frameworks enhance trust in Internet enabled infrastructure and services, facilitate digital trade, and help protect users and service providers.

As a competitive free market economy with well-established regulatory, legal and institutional structures, Australia has shared best practice and has continued the development of telecommunications policy and regulatory approaches with regional partners. This has occurred through our involvement in regional forums such as the APEC Telecommunications and Information Working Group and through bilateral exchanges (*see Vanuatu's Regulatory Environment Supporting Greater Connectivity, page 74*).

ENABLING ACCESS TO THE INTERNET

The private sector plays a crucial role in enabling access to the Internet. Most of the base infrastructure used for Internet access and connectivity is maintained and operated by the private sector. This infrastructure generates new markets for companies and digital products and services, while underpinning socio-economic development in those markets.

VANUATU'S REGULATORY ENVIRONMENT SUPPORTING GREATER CONNECTIVITY

The Australian Aid program, *Governance for Growth* (GFG), supported liberalisation of Vanuatu's telecommunications sector. The program provided assistance to the government to break the monopoly held by Telecom Vanuatu Limited, in part through establishing the Office of the Telecommunications and Radio Communications Regulator. This led to the introduction of Digicel as an alternative telecommunications service provider. As a result, mobile penetration has increased from 27 per cent of Vanuatu's population in 2008 to over 80 per cent in 2016.

The GFG program also assisted the Vanuatu Government to establish the Office of the Government Chief Information Officer (OGCIO). In 2014, the OGCIO developed a Universal Access Policy, which compels telecommunications service providers to expand coverage to 98% of the country by 1 January 2018. This has contributed to a significant increase in availability and affordability of broadband Internet services throughout Vanuatu.

AUSTRALIA WILL:

7.01 Partner with international organisations, regional governments, development banks and the private sector to improve Internet accessibility in the Indo-Pacific

7.02 Work with partner countries in the Indo-Pacific to develop domestic regulatory, legal and institutional frameworks that support competitive telecommunications sectors

7.03 Promote digital inclusion across the Indo-Pacific through educational programs, leadership initiatives and strategic partnerships

Encourage the use of resilient development-enabling technologies

The role of digital technologies as enablers of development is expanding. Inclusive access to digital technologies is critical to ensure that all individuals can more readily enjoy the benefits of increasingly digital societies.

E-GOVERNANCE AND DIGITAL DELIVERY OF SERVICES

Access to digital information and services empowers individuals. It opens new channels through which people can engage financially, socially and politically. Increasingly, core services including banking and finance, education and healthcare are most effectively accessed using digital technologies (see *The Tupaia Initiative and Digital Delivery of Services, page 76*).

E-governance – the delivery of government services through online platforms – can improve administration processes, service delivery, government accountability and transparency. Australia recognises the transformative role that digital technologies play in increasing the efficiency and effectiveness of government services.

Beyond this, digital technologies also provide alternative solutions to challenges. Australia has played a role in enhancing school attendance and educational outcomes across the region by providing digital reporting and lesson-planning tools to teachers and schools. Australia has contributed to the empowerment of women and girls in the region through deploying technology and training to young women, enhancing their digital inclusion and financial independence.

'By reducing information costs, digital technologies greatly lower the cost of economic and social transactions for firms, individuals, and the public sector. They promote innovation when transaction costs fall to essentially zero. They boost efficiency as existing activities and services become cheaper, quicker, or more convenient. And they increase inclusion as people get access to services that previously were out of reach.'

Digital Dividends, The World Bank, 2016.

THE TUPAIA INITIATIVE AND DIGITAL DELIVERY OF SERVICES

Australia's Department of Foreign Affairs and Trade's *innovationXchange* is investing an initial $2 million in a collaboration with software providers to transform the availability of medical supply information across the Pacific Islands. This investment will supply partner governments with an easy to use digital dashboard showing real time essential medical supply information.

Health planners and other key decision-makers within local health systems will know where their medical supplies are stored and frontline nursing and pharmaceutical staff will be able to place and track their orders, enhancing availability of medical supplies in the areas where they are needed most.

INNOVATIVE USES OF TECHNOLOGY FOR FINANCIAL INCLUSION

Engagement in the formal financial sector is a catalyst for inclusive economic growth and sustainable development. It is difficult to pinpoint exact numbers of people in the Indo-Pacific who do not engage the services of a bank or similar financial institution, but the numbers are significant. We know that over 400 million people in Southeast Asia alone remain 'unbanked'. Increased participation by the APEC region in the formal financial sector will increase the region's economic contribution from $17 billion to $52 billion by 2030.

New technologies give rise to new opportunities for financial inclusion. Formalising banking by increasing access to online and mobile banking and e-financing arrangements (such as Government-to-Person digital payment systems in the Indo-Pacific) will reduce administration costs for governments and businesses, make savings more secure and increase financial inclusion, especially for women and girls and people living in rural and remote areas.

As current co-chair of the G20 *Global Partnership for Financial Inclusion Subgroup on Markets and Payment Systems* (alongside Mexico), Australia is engaged in promoting digital payment systems and providing secure, cost-effective digital financial services and products. The Subgroup's *Guidance Note on Building Inclusive Digital Ecosystems* has been a key outcome of Australia's 2017 co-chairmanship. This Guidance Note supports the implementation of inclusive digital payment systems and the provision of safe, cost-effective digital financial services and products.

PRIVATE SECTOR ENGAGEMENT

Alongside government, the private sector has an important stake in the digital inclusion of countries and populations across the Indo-Pacific. Financial institutions and service providers are increasingly using digital technologies to enhance delivery of their financial products and services.

CYBER SECURITY FOR RESILIENT TECHNOLOGY-ENABLED DEVELOPMENT

Greater connectivity has the potential to facilitate sustainable and inclusive development. However, it also brings new threats. Poor cyber security practices and low cybercrime awareness can undermine trust in cyberspace, reducing the dividends of digital technologies. Conversely, trust in the online environment sustains and extends the development-enabling capacity of digital technologies.

Australian development projects will take into account the long-term security and resilience of technologies. This will support the safety and privacy of users and build trust in online systems. Technologies that are known to be resilient to threats, and that are trusted by users, will have greater impact on development outcomes.

AUSTRALIA WILL:

7.04 Work with partner governments, the private sector and financial institutions across the Indo-Pacific to promote e-governance, online service delivery and innovative uses of technology for enhanced economic opportunity and sustainable development

7.05 Provide guidance to ensure that digital technologies used or provided in Australian aid and non-government projects are safe and resilient

Support entrepreneurship, digital skills and integration into the global marketplace

The introduction of new digital technologies will continue to act as a catalyst for development, but technological advancements can also disrupt traditional economic and labour markets. Innovative uses of technology by individuals, entrepreneurs, governments and businesses can harness digital disruption for good, upskilling workers and integrating people and economies into the global marketplace. Australia is committed to bridging digital divides within and between countries in the region by bolstering entrepreneurship, digital-ready workforces and inclusive digital trade.

ENCOURAGING INNOVATION AND ENTREPRENEURSHIP

Innovation and entrepreneurship are critical factors in sustaining an open, free and secure cyberspace. Innovators develop new ways for people to participate and collaborate online. Entrepreneurs take new ideas forward and enhance access to and use of the Internet. Together, these activities ensure that cyberspace remains an ever-evolving force for inclusive economic growth and sustainable development.

Australia supports public-private innovation challenges that search for innovative and entrepreneurial solutions to development challenges across the region (*see CSIRO ON Prime Accelerator Program*). Australia's Ambassador for Cyber Affairs will host a *Technology for Development Challenge* for entrepreneurs and start-ups from Australia and the Indo-Pacific to find innovative technology-based solutions to regional development challenges.

CSIRO ON PRIME ACCELERATOR PROGRAM

CSIRO's ON Prime Accelerator Program is working with the Department of Foreign Affairs and Trade to explore ways in which technologies that have the potential to deliver gains in connectivity, online service delivery and data collection across the Indo-Pacific can be maximised. *ON Prime* is an entry level, part-time pre-accelerator that helps teams validate their research through a process of customer discovery and market validation, and discover a real world application for it. Going forward, the aim is to encourage teams with research in this space to discover the value of their work and maximize their potential impact.

AUSTRALIA WILL:

7.06 Work with public and private sector partners to encourage businesses and entrepreneurs to find solutions to regional development challenges using innovative technologies

DIGITAL-READY WORKFORCES

In order to realise the potential of the digital age, populations must be digitally skilled. Some countries in the Indo-Pacific have highly skilled digital-ready workforces. In many others, however, digital literacy and skills vary greatly among working populations. An absence of digital skills and technical expertise holds people back from participating fully in the digital economy.

As technology becomes increasingly available, demand for digitally literate workers will continue to expand. In order to prepare populations for increasingly digitalised jobs, schools, universities and training programs for working age and older persons must equip people with digital skills. In addition to traditional education, agile approaches to bridging skills gaps are needed across the region. Governments and businesses have a shared and growing need to work together in this area to build up digital-ready workforces.

Australia's Department of Foreign Affairs and Trade's *innovationXchange* is working with private sector and university partners to source solutions to digital skills shortages across the region. Grant funding will be awarded to project proposals that will upskill Indo-Pacific populations, especially young people, women and girls, and people with disabilities.

Digitally skilled populations will themselves become catalysts for inclusive economic growth and sustainable development. Groups previously underrepresented in the digital landscape will gain the skills needed to access jobs, expanded economic opportunities, information, government services and social engagement online.

AUSTRALIA WILL:

7.07 Partner with regional governments, multilateral forums and educational institutions to build digital-ready workforces and support digital upskilling across the Indo-Pacific

INTEGRATION INTO THE GLOBAL MARKETPLACE

Through its ongoing *Aid for Trade* program, Australia helps individuals, businesses and economies integrate into the global marketplace. Encouraging growth of digital trade delivers particular benefits to small businesses, women and girls, low-income groups, indigenous, ethnic and religious minorities, and others.

Australia has committed $10 million to multilateral programs that assist developing countries to undertake trade facilitation reform. This includes the World Bank's *Trade Facilitation Support Program*, World Trade Organization (WTO) *Trade Facilitation Agreement Facility*, and the *Global Alliance for Trade Facilitation*. In 2015, Australia endorsed the G20 *Digital Economy Development and Cooperation Initiative*, which seeks to improve digital trade outcomes, including for developing countries and vulnerable groups.

AUSTRALIA WILL:

7.08 Support new technologies and tools for developing countries to facilitate trade, including improvements in policy and customs practices and better access to trade finance

7.09 Focus Australian Aid for Trade efforts on connecting small businesses and women entrepreneurs in developing countries to digital economy opportunities and global supply chains

SHAPING INCLUSIVE FINANCE TRANSFORMATIONS IN ASEAN

Australia's ASEAN and Mekong regional aid program is supporting increased participation in digital trade. For example, the *Shaping Inclusive Finance Transformations* in ASEAN investment (SHIFT, $9.9 million, 2014–2018, implemented by the United Nations Capital Development Fund - UNCDF), is developing innovative digital services to help low-income women and men access financial services. SHIFT supported development of LienVietPostBank's new e-wallet. This offers the full array of low-cost banking services via a client's smartphone, supporting low-income people in Vietnam gain financial independence and growing a new market for financial services.

COMPREHENSIVE & COORDINATED CYBER AFFAIRS

AUSTRALIA'S GOAL:

Australia pursues a comprehensive & coordinated cyber affairs agenda

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- **Enhance** understanding of Australia's comprehensive cyber affairs agenda
- **Increase** funding for Australia's international cyber engagement activities
- **Coordinate** and prioritise Australia's international cyber engagement activities

The digital age presents a diverse range of opportunities and challenges for Australia. This Strategy captures the breadth of Australia's agenda for cyber affairs through its seven thematic chapters: *Digital Trade*, *Cyber Security*, *Cybercrime*, *International Security & Cyberspace*, *Internet Governance & Cooperation*, *Human Rights & Democracy Online* and *Technology for Development*.

The borderless nature of cyberspace means that the capacity and behaviour of other states, the private sector, civil society and individuals can affect Australia's cyber interests. Cyber diplomacy and outreach is essential to promoting and protecting Australia's national security, foreign policy, economic and trade interests, as well as our development objectives.

Australia's various cyber interests are all deeply interconnected. For example, increased internet penetration resulting from development projects promotes inclusive economic growth, while helping more people get online in the Indo-Pacific boosts our regional economy, creating new opportunities for Australia's private sector to market their digital goods and services.

Australia will work closely with international partners, both in the Indo-Pacific and across the globe, to pursue our cyber affairs agenda. Reflecting differing levels of connectivity and digital development in the region, our partners offer varying opportunities for engagement and collaboration. Some countries with particular expertise and capabilities will be key partners in the practical delivery of Australia's cyber affairs agenda, while others will be key beneficiaries.

As our neighbours become more connected, Australia will partner to build their technical, legislative and institutional capacity to fight cybercrime. This will not only preserve our neighbours' economic growth, but also prevent the creation of cybercrime safe havens that could be used to target Australians. Such capacity building also equips countries to participate more constructively in international discussions on the future of cyberspace. At the same time, investing in capacity building and improving international collaboration on shared cyber challenges helps to ensure that Australia and Australians can enjoy the benefits of cyberspace, while mitigating the risks.

In different combinations, Australia's cyber interests either reinforce each other or require conscious balancing. For example, overcoming barriers to development and successfully addressing cybercrime both improve the performance of the digital economy. In contrast, pursuing digital development without addressing the risk of cybercrime could be counterproductive. Similarly, chasing absolute security without considering the benefits of digital trade could lead to missed opportunities. Australia will reconcile the complex relations between these various factors by pursuing a comprehensive and coordinated approach to cyber affairs.

In recognising the significance of cyber affairs to our national interest, Australia will increase the understanding, funding and coordination of our international cyber engagement. Greater resources and a harmonised approach to international cyber engagement will ensure Australia achieves its goals in cyberspace.

Collaborating and cooperating with the private sector, civil society, academia and other governments will be vital to ensure that Australia's fundamental objective of an open, free and secure Internet is achieved.

Enhance understanding of Australia's comprehensive cyber affairs agenda

Cyber issues cut across almost all areas of Australia's international engagement. The prominence of these issues will continue to grow as global connectivity and technology uptake continue to increase. In acknowledgement of this, Australia will work to improve understanding of its comprehensive international cyber agenda amongst all stakeholders, both domestic and international.

Australia embraces a holistic idea of 'cyber capacity'. This includes a state's ability to: ensure people's rights online; achieve economic growth through digital trade; combat cybercrime; and engage in conversations about Internet governance and international security in cyberspace.

Australia will bring conversations concerning development assistance and cyber security capacity together, reconciling the goals, priorities and terminology discussed. Similarly, cyber capacity building will encompass important elements beyond purely technical training, including policy and legislation, education and infrastructure.

FIGURE 1: Australia's interconnected cyber affairs interests

This Strategy conveys Australia's comprehensive cyber affairs vision to the international community. This vision will be reinforced through Australia's ongoing diplomatic engagements, and will also be promoted to domestic stakeholders through regular consultation across the Australian Government and industry.

In order to deliver Australia's comprehensive cyber affairs agenda internationally, Australia needs those who represent the country to be equipped with an in-depth understanding of international cyber issues and Australia's interests in cyberspace. Australia will develop a Cyber Affairs Curriculum for its Diplomatic Academy. Courses will provide Australia's international representatives from across government with a detailed view of our cyber affairs agenda. The material will cover Australia's national security, foreign policy, economic and trade interests, and legal and development objectives regarding the Internet and cyberspace. 'Workshops in a box' – curriculums that can be delivered to representatives already on international postings – will further disseminate cyber affairs awareness. This will ensure that Australia's international cyber affairs agenda is not only comprehensive in concept, but also broad in stewardship.

Empowering the people at the forefront of Australia's international cyber engagement will be the foundation of Australia's coordinated approach to cyber affairs.

AUSTRALIA WILL:

8.01 Promote Australia's comprehensive vision of cyber affairs through ongoing diplomatic engagement

8.02 Create a Cyber Affairs Curriculum for Australia's international representatives through DFAT's Diplomatic Academy

Increase funding for Australia's international cyber engagement activities

Australia's newly established *Cyber Cooperation Program*, announced by the Foreign Minister in May 2016, is designed to boost the resources behind Australia's cyber capacity building efforts. Projects funded by the Program will encompass the full spectrum of cyber affairs, whether that be raising the bar of cyber security, cybercrime capacity building, or pursuing economic and development goals.

While introduced with an initial investment of $1 million per year over four years, in recognition of the growing importance of this field, the Government has supplemented this funding with an additional $10 million over three years, taking the total investment to $14 million. This additional investment ensures that the priorities outlined in this Strategy can be delivered through practical action.

The Indo-Pacific will be the focus area of the Program's projects. This is where our capacity building efforts will have the greatest impact and translate most directly into gains for Australia. Australia will work with partners who have a well-established capability and complementary objectives. In this way, we will harness the existing capacity of the Indo-Pacific to deliver greater outcomes to the region as a whole, including to those countries who are at the beginning of their digital journey.

Australia will actively seek creative partnering opportunities with governments around the world and with civil society, academia and the private sector. Our combined resources, networks and expertise will be a force multiplier in pursuit of shared goals. The *Cyber Cooperation Program* will provide the support for many of the new international cyber engagement activities in the Strategy.

AUSTRALIA WILL:

8.03 Fund new international cyber engagement projects in the Indo-Pacific through the Cyber Cooperation Program

Coordinate and prioritise Australia's international cyber engagement

The breadth of Australia's comprehensive cyber affairs agenda means that there are many stakeholders across government who promote and safeguard Australia's international interests in cyberspace. The growing profile of these issues and Australia's increasing investment means it is becoming even more important to ensure that all of Australia's international cyber activities are effectively coordinated.

The Ambassador for Cyber Affairs will coordinate and prioritise Australia's international cyber engagement across the full spectrum of international cyber affairs.

Recognising that important work is already going on across Government, the Ambassador for Cyber Affairs will convene a quarterly whole-of-Government International Cyber Engagement Group. The Group will bring together all Government representatives with a stake in Australia's cyber affairs. This will help amplify the visibility of existing efforts, increase useful cross-departmental collaborations, avoid duplications of effort, and ensure an overarching direction and prioritisation.

As foreshadowed in the *Digital Trade chapter*, Australia will engage with a new dedicated private sector advisory body that will consult directly with the Government on international cyber issues. The Industry Advisory Group will provide the practical framework for Australia's public-private partnership on cyber issues and ensure that the Government collaborates with the private sector in pursuit of its cyber affairs agenda.

By adopting a comprehensive approach, boosting funding and increasing coordination of international cyber engagement across Government, civil society, academia and the private sector, Australia will ensure its prosperity and security in cyberspace.

AUSTRALIA WILL:

8.04 Establish a quarterly whole-of-Government meeting, convened by the Ambassador for Cyber Affairs, to coordinate and prioritise Australia's international cyber activities

8.05 Establish an Industry Advisory Group that meets biannually to facilitate public-private collaboration on Australia's international cyber engagement

ANNEXES

Annex A: Australia's position on how international law applies to state conduct in cyberspace

Existing international law provides the framework for state behaviour in cyberspace. This includes, where applicable, the law regarding the use of force, international humanitarian law (IHL), international human rights law, and international law regarding state responsibility.

In this respect, Australia notes that the centrality of international law and its application to states' use of cyberspace was affirmed in 2013 in the consensus report of the third *United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, which was chaired by Australia, and reaffirmed in the 2015 report of the UNGGE.

However, Australia recognises that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty, attribution and jurisdiction, given that different actors engage in a range of cyber activities which may cross multiple national borders. This annex sets out Australia's views on these issues.

1. The United Nations Charter and the law on the use of force (*jus ad bellum*) apply to activities conducted in cyberspace.

The Charter of the United Nations requires states to seek peaceful settlements of disputes. This obligation extends to cyberspace and requires states to resolve cyber incidents peacefully without escalation or resort to the threat or use of force. This requirement does not impinge upon a state's inherent right to act in individual or collective self-defence in response to an armed attack, which applies equally in the cyber domain as it does in the physical realm.

In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning.

2. For cyber operations constituting or occurring within the context of an international or non-international armed conflict, the relevant international humanitarian law (*jus in bello*) will apply to the conduct of these cyber activities.

International humanitarian law (IHL) (including the principles of humanity, necessity, proportionality and distinction) applies to cyber operations within an armed conflict.

The IHL principle of proportionality prohibits the launching of an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or

a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

The IHL principle of military necessity states that a combatant is justified in using those measures, not forbidden by international law, which are indispensable for securing complete submission of an enemy at the soonest moment. The principle cannot be used to justify actions prohibited by law, as the means to achieve victory are not unlimited.

The IHL principle of distinction seeks to ensure that only legitimate military objects are attacked. Distinction has two components. The first, relating to personnel, seeks to maintain the distinction between combatants and non-combatants or military and civilian personnel. The second component distinguishes between legitimate military targets and civilian objects.

All Australian military capabilities are employed in line with approved targeting procedures. Cyber operations are no different. Australian targeting procedures comply with the requirements of IHL and trained legal officers provide decision-makers with advice to ensure that Australia satisfies its obligations under international law and its domestic legal requirements.

For example, Australia considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack under IHL', the rules governing such attacks during armed conflict will apply to those kinds of cyber operations.

3. For cyber activities taking place outside of armed conflict, general principles of international law, including the law on state responsibility, apply.

It is a longstanding rule of international law that, if a state acts in violation of an international obligation, and that violation is attributable to the state, that state will be responsible for the violation.

The customary international law on state responsibility, much of which is reflected in the International Law Commission's *Articles on the Responsibility of States for Internationally Wrongful Acts*, apply to state behaviour in cyberspace.

To the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states. In this context, we note it may not be reasonable to expect (or even possible for) a state to prevent all malicious use of ICT infrastructure located within its territory. However, in Australia's view, if a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law.

If a state is a victim of malicious cyber activity which is attributable to a perpetrator state, the victim state may be able to take countermeasures against the perpetrator state, under certain circumstances. However, countermeasures that amount to a use of force are not permissible. Any use of countermeasures involving cyberspace must be proportionate. It is acknowledged that this raises challenges in identifying and assessing direct and indirect effects of malicious cyber activity, in order to gauge a proportionate response. The purpose of countermeasures is to compel the other party to desist in the ongoing unlawful conduct.

Annex B: Norms for the responsible behaviour of states in cyberspace

From the report of the 2015 *UN Group of Government Experts* on *Development in the Field of Information and Telecommunications in the Context of International Security* (A/70/174).

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Annex C: International cyber engagement strategy action plan

DIGITAL TRADE

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Shape an enabling environment for digital trade including through trade agreements, harmonisation of standards, and implementation of trade facilitation measures	
1.01 Advocate for further digital trade liberalisation and facilitation through free trade agreements and through Australia's participation in the WTO, OECD, APEC and G20 **ONGOING**	DFAT
1.02 Support capacity building projects in the Indo-Pacific to encourage the harmonisation of international standards for digital goods, building trust and confidence in digital trade **MEDIUM TERM**	DIIS DFAT (Standards Australia)
1.03 Oppose barriers to digital trade and advocate for implementation of the WTO Trade Facilitation Agreement through bilateral representations and involvement with WTO committees and councils, APEC and the G20 **ONGOING**	DFAT
1.04 Design and trial an electronic Secure Trade Lane with New Zealand to provide benefits for trusted traders in both countries **MEDIUM TERM**	DIBP
1.05 Promote regulatory cooperation and coherence through Australia's bilateral exchanges, the Australian free trade agreement agenda, Aid for Trade activities, and engagement in the G20 and APEC **ONGOING**	DFAT ASIC

Australia's Actions	Lead Agency
1.06 Support public-private engagement on emerging digital trade issues in multilateral forums, including the Business 20, G20, and the APEC Business Advisory Council **ONGOING**	DFAT DIIS
1.07 Support the G20, OECD and other international research to improve digital trade measurement and develop policy responses **MEDIUM TERM**	DFAT DIIS
1.08 Encourage transparency from bilateral partners on domestic legislation that could restrict trade, including through cyber policy dialogues **ONGOING**	DFAT Austrade DIIS
AUSTRALIA'S PRIORITY Promote trade and investment opportunities for Australian digital goods and services	
1.09 Develop a guide to exporting in the digital economy, providing practical advice for maximising international opportunities for Australian businesses **SHORT TERM**	Austrade DIIS
1.10 Develop a national digital economy strategy, which will position Australia to embrace the opportunities presented by digital trade **SHORT TERM**	DIIS Austrade

CYBER SECURITY

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Maintain strong cyber security relationships with international partners	
2.01 Strengthen and expand Australia's international cyber security information sharing partners and trusted networks **ONGOING**	ACSC
2.02 Strengthen and expand Australia's network of CERT relationships, especially in the Indo-Pacific **ONGOING**	CERT Australia ACSC DoCA
2.03 Be a prominent contributor to the APCERT community **ONGOING**	CERT Australia ACSC
AUSTRALIA'S PRIORITY Encourage innovative cyber security solutions and deliver world leading cyber security advice	
2.04 Promote cyber security as a fundamental input in the design and delivery of ICT products, systems and services **ONGOING**	ACSC
2.05 Support the development of international standards that improve cyber security and encourage harmonisation of standards for digital products **ONGOING**	(Standards Australia) ACSC

Australia's Actions	Lead Agency
2.06 Publish translations of ASD's Essential Eight strategies and companion implementation documents in the official languages of ASEAN members **SHORT TERM**	ACSC DFAT
AUSTRALIA'S PRIORITY Develop regional cyber security capability	
2.07 Work with regional partners in the Pacific to establish the Pacific Cyber Security Operational Network (PaCSON) **MEDIUM TERM**	CERT Australia
AUSTRALIA'S PRIORITY Promote Australia's cyber security industry	
2.08 Showcase Australia's cyber security capabilities to international customers and investors, including through delivery of an annual Australian Cyber Week **LONG TERM**	(AustCyber) DIIS
2.09 Promote and encourage cyber security start-ups through Landing Pads **ONGOING**	Austrade (AustCyber)
2.10 Partner with the private sector to host a workshop to co-design how Australia promotes its cyber security industry internationally **SHORT TERM**	(AustCyber) Austrade DIIS

CYBERCRIME

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Raise cybercrime awareness in the Indo-Pacific	
3.01 Deliver cybercrime awareness training across the Indo-Pacific through public-private partnerships and the refreshed Cyber Safety Pasifika program **SHORT TERM**	AFP
AUSTRALIA'S PRIORITY Assist Indo-Pacific countries to strengthen their cybercrime legislation	
3.02 Promote the Budapest Convention as a best practice model for legislative responses to cybercrime and support accession to the Convention across the Indo-Pacific **ONGOING**	DFAT AGD AFP
3.03 Be active in the negotiation of an Additional Protocol to the Budapest Convention on trans-border access to information **MEDIUM TERM**	AGD
3.04 Work with the Pacific Islands Law Officers' Network to help strengthen cybercrime legislation in the region **ONGOING**	AGD DFAT
AUSTRALIA'S PRIORITY Deliver cybercrime law enforcement and prosecution capacity building in the Indo-Pacific	

Australia's Actions	Lead Agency
3.05 Provide cybercrime training to law enforcement officers, prosecutors and judges across the Indo-Pacific **ONGOING**	AFP DFAT AGD
AUSTRALIA'S PRIORITY Enhance diplomatic dialogue and international information sharing on cybercrime	
3.06 Seek further opportunities to participate in strategic-level engagement on combatting transnational cybercrime **SHORT TERM**	DFAT
3.07 Share cybercrime threat information and enhance operational collaboration with international partners to fight transnational crime **ONGOING**	AFP ACIC AUSTRAC

INTERNATIONAL SECURITY & CYBERSPACE

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Set clear expectations for state behaviour in cyberspace	
4.01 Periodically publish Australia's position on the application of relevant international law to state conduct in cyberspace (the first such publication is in Annex A) **ONGOING**	DFAT AGD
4.02 Facilitate advanced policy development and promote informed public discussion on acceptable state behaviour in cyberspace through engagement with academics and experts in this field **ONGOING**	DFAT AGD Defence
4.03 Seek high-level reaffirmations from states that they will act in accordance with international law and identified norms of responsible state behaviour in cyberspace **ONGOING**	DFAT
4.04 Partner with countries in the Indo-Pacific to advance our combined understanding of how international law and norms of responsible state behaviour apply in cyberspace through bilateral engagement and regional and multilateral forums **ONGOING**	DFAT
AUSTRALIA'S PRIORITY Implement practical confidence building measures to prevent conflict	
4.05 Develop a framework to exchange policy and diplomatic contacts, including bilaterally, to facilitate communication in times of crisis or tension arising from significant cyber incidents that have the potential to threaten international peace, security and stability **MEDIUM TERM**	DFAT ACSC

Australia's Actions	Lead Agency
4.06 Work with regional organisations to conduct risk reduction workshops to enhance our capacity to manage and respond to cyber incidents that threaten international peace, security and stability, including exercising national and regional responses to severe cyber incidents **SHORT TERM**	DFAT ACSC
4.07 Hold cyber policy dialogues to discuss and work with partners to achieve priority goals on international cyber issues, including international law, norms of responsible state behaviour and confidence building measures **ONGOING**	DFAT
4.08 Foster recognition through diplomatic outreach and defence engagement that military offensive cyber capabilities are subject to the same limitations and obligations as any other military capability **ONGOING**	DFAT Defence ASD
AUSTRALIA'S PRIORITY Deter and respond to unacceptable behaviour in cyberspace	
4.09 Review Australia's range of options to deter and respond to unacceptable behaviours in cyberspace, particularly those involving state actors and their proxies **MEDIUM TERM**	PM&C DFAT AGD ASD
4.10 Undertake diplomatic action to support an international cooperative architecture that promotes stability and responds to and deters unacceptable behaviour in cyberspace **MEDIUM TERM**	DFAT

INTERNET GOVERNANCE & COOPERATION

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Advocate for a multi-stakeholder approach to Internet governance that is inclusive, consensus-based, transparent and accountable	
5.01 Advocate for an open, free and secure Internet, underpinned by a multi-stakeholder approach to Internet governance and cooperation **ONGOING**	DFAT DoCA
5.02 Support an annual community-led Australian Internet governance and cooperation forum **SHORT TERM**	DoCA DFAT
5.03 Outline Australia's strong commitment to fostering fair and effective competition online, emphasising a preference for general competition law **ONGOING**	DoCA ACCC DFAT
AUSTRALIA'S PRIORITY Oppose efforts to bring the management of the Internet under government control	
5.04 Oppose efforts to bring the management of the Internet under government control **ONGOING**	DoCA DFAT
AUSTRALIA'S PRIORITY Raise awareness across the Indo-Pacific of Internet governance issues and encourage engagement of regional partners in Internet governance and cooperation discussions	
5.05 Build the capacity of Indo-Pacific partners to engage in regional and international discussion on Internet governance and cooperation **MEDIUM TERM**	DoCA DFAT

HUMAN RIGHTS & DEMOCRACY ONLINE

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Advocate for the protection of human rights and democratic principles online	
6.01 Advocate to uphold and protect human rights and democratic freedoms online **ONGOING**	DFAT DoCA
6.02 Share concerns about, and aim to prevent, undue restrictions of human rights online as well as cyber-enabled interference in democratic processes **ONGOING**	DFAT
6.03 Fund capacity building in the Indo-Pacific to raise awareness of states' human rights obligations online **MEDIUM TERM**	DFAT
AUSTRALIA'S PRIORITY Support international efforts to promote and protect human rights online	
6.04 Support non-government organisations that defend human rights online **MEDIUM TERM**	DFAT
AUSTRALIA'S PRIORITY Ensure respect for and protection of human rights and democratic principles online are considered in all Australian aid projects with digital technology components	
6.05 Provide guidance to ensure that human rights online are protected in Australian aid and non-government projects with digital technology components **SHORT TERM**	DFAT

TECHNOLOGY FOR DEVELOPMENT

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Improve connectivity and access to the Internet across the Indo-Pacific, in collaboration with international organisations, regional governments and the private sector	
7.01 Partner with international organisations, regional governments, development banks and the private sector to improve Internet accessibility in the Indo-Pacific **LONG TERM**	DFAT DoCA
7.02 Work with partner countries in the Indo-Pacific to develop domestic regulatory, legal and institutional frameworks that support competitive telecommunications sectors **MEDIUM TERM**	DFAT DoCA
7.03 Promote digital inclusion across the Indo-Pacific through educational programs, leadership initiatives and strategic partnerships **LONG TERM**	DFAT
AUSTRALIA'S PRIORITY Encourage the use of resilient development-enabling technologies for e-governance and the digital delivery of services	
7.04 Work with partner governments, the private sector and financial institutions across the Indo-Pacific to promote e-governance, online service delivery and innovative uses of technology for enhanced economic opportunity and sustainable development **MEDIUM TERM**	DFAT Austrade

Australia's Actions	Lead Agency
7.05 Provide guidance to ensure that digital technologies used in, or provided to, Australian aid and non-government projects are safe and resilient **SHORT TERM**	DFAT
AUSTRALIA'S PRIORITY Support entrepreneurship, digital skills and integration into the global marketplace	
7.06 Work with public and private sector partners to encourage businesses and entrepreneurs to find solutions to regional development challenges using innovative technologies **SHORT TERM**	DFAT (AustCyber) Austrade CSIRO
7.07 Partner with regional governments, multilateral forums and educational institutions to build digital-ready workforces and support digital upskilling across the Indo-Pacific **SHORT TERM**	DFAT
7.08 Support new technologies and tools for developing countries to facilitate digital trade, including improvements in policy and customs practices and better access to trade finance **MEDIUM TERM**	DFAT DIIS
7.09 Focus Australian Aid for Trade efforts on connecting small businesses and women entrepreneurs in developing countries to digital economy opportunities and global supply chains **ONGOING**	DFAT Austrade

COMPREHENSIVE & COORDINATED CYBER AFFAIRS

Australia's Actions	Lead Agency
AUSTRALIA'S PRIORITY Enhance understanding of Australia's comprehensive cyber affairs agenda	
8.01 Promote Australia's vision of comprehensive cyber affairs through ongoing diplomatic engagement **ONGOING**	DFAT
8.02 Create a Cyber Affairs Curriculum for Australia's international representatives through DFAT's Diplomatic Academy **SHORT TERM**	DFAT
AUSTRALIA'S PRIORITY Increase funding for Australia's international cyber engagement activities	
8.03 Fund new international cyber engagement projects in the Indo-Pacific through the Cyber Cooperation Program **ONGOING**	DFAT
AUSTRALIA'S PRIORITY Coordinate and prioritise Australia's international cyber engagement activities	
8.04 Establish a quarterly whole-of-Government meeting, convened by the Ambassador for Cyber Affairs, to coordinate and prioritise Australia's international cyber activities **SHORT TERM**	DFAT
8.05 Establish an Industry Advisory Group that meets biannually to facilitate public-private collaboration on Australia's international cyber engagement **SHORT TERM**	DFAT Austrade DIIS CERT Australia

Australian Government