
AUSTRALIA'S
INTERNATIONAL CYBER
AND CRITICAL TECH
ENGAGEMENT STRATEGY

AUSTRALIA'S INTERNATIONAL CYBER AND CRITICAL TECH ENGAGEMENT STRATEGY

Australian Government

ISBN

ISBN 978-1-74322-553-0 Australia's International Cyber and Critical Tech Engagement Strategy (PDF)
ISBN 978-1-74322-554-7 Australia's International Cyber and Critical Tech Engagement Strategy (Book [softcover])

Attribution

This publication should be attributed as follows: Commonwealth of Australia, Department of Foreign Affairs and Trade, Australia's International Cyber and Critical Technology Engagement Strategy, 2021

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website: https://www.pmc.gov.au/resource-centre/government/commonwealth-coat-arms-information-and-guidelines

Website

https://www.internationalcybertech.gov.au

Contact

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

Cyber Affairs and Critical Technology Branch
Department of Foreign Affairs and Trade
RG Casey Building, John McEwen Crescent
Barton ACT 0221

CONTENTS

Foreign Minister's Foreword

Technology is changing the way we live, work and interact faster than ever. New technologies are proliferating, widening the scope of economic transformation and disrupting social, legal and political systems.

The Indo-Pacific region is undergoing the most significant shift in strategic alignment in the modern era. Factors such as increasing competition between major powers, and the adoption and integration of technology-enabled grey zone activities into statecraft mean Australia is facing a more dynamic and contested regional environment.

Existing and emerging critical technologies will drive more efficient and productive economies, help respond to future pandemics and health crises, and support more sustainable and equitable global development. Applications of Artificial Intelligence (AI) can increase productivity in ways that will add trillions of dollars to the global economy, and through applications such as earlier diagnosis of disease, will create better health outcomes. Increased digital connectivity provides communities with greater opportunities for education, access to government services and economic participation.

However, the promise of technology comes with new risks. As our reliance on technology increases, new means to misuse it are being developed. This includes unlawful invasive surveillance, malign influence operations using disinformation, and new ways to control populations and conduct foreign interference including political and economic coercion. The misuse of technology has exacerbated social divisions and inequality, and has been used to promote messages of hate and terror. Countries and companies at the cutting edge of innovation in these critical technologies often promote values that are at odds with our own.

Since the release of the *International Cyber Engagement Strategy in 2017*, Australia has strengthened its reputation as a world leader in engagement on cyber issues. The *International Cyber and Critical Technology Engagement Strategy* builds on this and expands our cyber-focused international engagement to add a broader perspective on critical technologies. This will not diminish our focus on international cyber policy, recognising that an open, free, safe and secure cyberspace is necessary for sustained technological innovation.

The *2021 International Cyber and Critical Technology Engagement Strategy* sets out Australia's vision for a safe, secure and prosperous Australia, Indo-Pacific region and world enabled by cyberspace and critical technology. It provides

a framework to guide Australia's international engagement across the spectrum of cyber and critical technology issues in support of this vision, and the practical actions Australia will take to advance our objectives.

The Australian Government defines critical technologies as those technologies with the capacity to significantly enhance, as well as pose risks to, Australia's national interests, including our prosperity, society and national security.

Cyberspace has become such a critical element of Australia's prosperity that many – if not all – of the information and communications technologies that underpin it are considered critical technologies.

Since 2017, the world's reliance on cyberspace has grown. The experience of COVID-19, in which millions of people around the world found themselves even more dependent on cyberspace for work, education, tele-health, shopping and social engagement, further highlights our reliance on digital connectivity.

Australia and our international friends, partners and allies must shape the design, development and use of technology to reflect our values and interests. If we fail, we face a more uncertain future and increasing difficulties in protecting our prosperity, security, and sovereignty.

Senator the Hon Marise Payne
Minister for Foreign Affairs
Minister for Women

Introduction by the Ambassador for Cyber Affairs and Critical Technology

Competition over technology is increasingly at the centre of international politics and foreign policy.

While states have always sought to use technology for competitive gain, the countries that can harness the current wave of innovation, mitigate its risks, and capitalise on its transformative powers will gain economic, political and security advantages. The countries that manage this best will be at the forefront of 21st century leadership.

The Strategy builds on the *2017 International Cyber Engagement Strategy (ICES)* by incorporating critical technology into Australia's international engagement. While many of the drivers and foundations in the *2017 ICES* remain relevant, our international engagement must expand to reflect the increasing interconnectedness between cyberspace and critical technology.

The Strategy was developed through a comprehensive and rigorous consultation process with key international and domestic stakeholders including Government, state and territory governments, industry, civil society and the research community.

We met with over 100 experts from over 70 organisations to discuss the trends shaping the strategic, geopolitical and technical environment.

Additionally, we undertook a public call for submissions to encourage interested stakeholders in Australia and overseas to provide input into the Strategy.

Strategic planning in a time of significant change and disruption is essential but inherently difficult. In the current environment, it is possible that some of the trends and issues identified in the Strategy will require further responses and actions. However, while our strategic environment may change and technological disruption may accelerate, the foundations of Australia's international engagement on cyber and critical technology will remain the same.

To adapt to changes in our environment, we will regularly review our international engagement objectives and priorities. We will pursue a coordinated, national strategic approach to ensure all stakeholders are involved. We will always make decisions in our national interest. We will always work with industry and civil society, as well as the international community, including those who do not necessarily share our views.

Dr. Tobias Feakin
Ambassador for Cyber Affairs
and Critical Technology

EXECUTIVE SUMMARY

The Australian Government's vision is for a safe, secure and prosperous Australia, Indo-Pacific and world enabled by cyberspace and critical technology.

The *2021 International Cyber and Critical Technology Engagement Strategy* sets out Australia's interests and goals in pursuit of this vision, and provides a framework to guide Australia's whole-of-Government international engagement across the spectrum of cyber and critical technology issues.

To achieve our vision and navigate an increasingly challenging international environment, Australia must prioritise and enhance our international cyber and critical technology diplomacy.

The Strategy sets out how the Australian Government will pursue a strategic and coordinated national approach to shape cyberspace and critical technology in line with our interests and values, and build our international reputation as a trusted and influential leader on cyber and critical technology issues.

CRITICAL TECHNOLOGIES

The Australian Government defines critical technologies as those technologies with the capacity to significantly enhance, or pose risks to, Australia's national interests, including our prosperity, social cohesion and national security.

This includes, but is not limited to, technologies (or applications of technologies) such as cyberspace, Artificial Intelligence (AI), 5G, Internet of Things (IOT), quantum computing and synthetic biology.

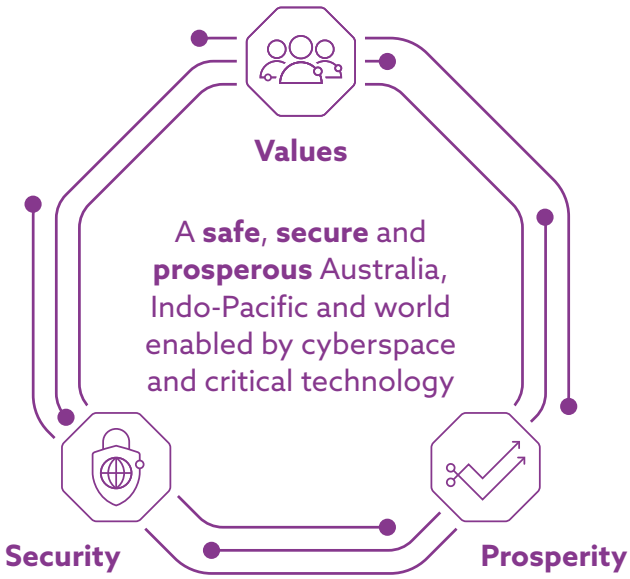
These, and other emerging technologies, will transform economic competitiveness, national and international security as well as democratic governance and social cohesion. These new technologies are often enabled by, and reliant on, information that is created, stored and transmitted through digital networks.

The Strategy identifies three main pillars – Values, Security and Prosperity – to guide Australia's international cyber and critical technology engagement (Refer to Figure 1).

- **Values** – We will always pursue a values-based approach to cyberspace and critical technology, and oppose efforts to use technologies to undermine these values.
- **Security** – We will always support international peace and stability, and secure, trusted and resilient technology.
- **Prosperity** – We will always advocate for cyberspace and technology to foster sustainable economic growth and development to enhance prosperity.

These pillars are interconnected and mutually reinforcing. Within these pillars sit 15 chapters. These chapters focus in detail on specific themes, and outline what actions Australia will take to protect and promote our interests in these areas. An Action Plan supports the strategy. The plan demonstrates the breadth of work and interests across the Australian Government on cyber and critical technology.

Figure 1



AT A GLANCE: AUSTRALIA'S INTERNATIONAL CYBER AND CRITICAL TECH ENGAGEMENT STRATEGY

Australia's goal: a **safe**, **secure** and **prosperous** Australia, Indo-Pacific and world enabled by cyberspace and critical technology

VALUES

Technology is used to uphold and protect liberal democratic values

- **Democratic Principles** - advocate for cyberspace and critical technologies to uphold and protect democratic principles and processes
- **Human Rights** - promote and protect human rights online and in the design, development and use of critical technologies
- **Ethics Of Critical Technology** - support the ethical design, development and use of critical technologies consistent with international law including human rights
- **Diversity & Gender Equality** - advocate for diversity, gender equality and women's empowerment in the design, development and use of cyberspace and critical technology

SECURITY

Secure, resilient and trusted technology

- **International Peace & Stability** - shape the development and use of critical technology, including cyberspace, to support international peace and stability
- **Disinformation & Misinformation** - build international resilience to digital disinformation and misinformation and their effects
- **Cyber Security** - build a strong and resilient cyber security capability for Australia, the Indo-Pacific and the world
- **Cybercrime** - strengthen cooperation for enhanced prevention, detection, investigation and prosecution of cybercrime
- **Online Harms & Safety** - enable a safe and inclusive online environment

PROSPERITY

Technology fosters sustainable economic growth and development

- **Regional Connectivity** - support a connected and prosperous Indo-Pacific comprised of independent sovereign states enabled by secure and economically viable critical technology
- **Markets & Supply Chains** - advocate for open, resilient, diverse and competitive international technology markets and supply chains
- **Research, Industry & Innovation** - strengthen Australian research, industry and innovation through international cooperation
- **Critical Technology Standards** - shape international critical technology standards that foster interoperability, innovation, transparency, diverse markets and security by design
- **Internet Governance** - promote the multi-stakeholder model of Internet governance
- **Digital Trade** - maximise economic growth by shaping an enabling environment for digital trade

CYBER AND CRITICAL TECHNOLOGY DIPLOMACY

Australia is a trusted and influential leader in cyber and critical technology diplomacy

CYBER AND CRITICAL TECHNOLOGY DIPLOMACY

Australia's goal: Australia is a trusted and influential leader in cyber and critical technology diplomacy

Australia will do this by:

Action 1. **Prioritising** and enhancing our cyber and critical technology diplomacy using a strategic and coordinated national approach

Action 2. **Shaping** the design, development and use of cyberspace and critical technology in line with Australia's interests and values

Action 3. **Enhancing** engagement with industry, civil society and the research community on cyberspace and critical technology

Cyberspace and critical technology affect all aspects of international relations. They underpin our national security, the protection and realisation of human rights and freedoms, global economic prosperity, sustainable development and international stability. To maintain, protect and strengthen our interests, we need to enhance our international engagement across the full spectrum of cyber and critical technology issues.

Australia is committed to ensuring cyberspace and critical technology enable a safe, secure and prosperous Australia, Indo-Pacific and world.

Yet we cannot take this outcome for granted. Growing strategic and technological competition is increasing the risks to international stability.

CRITICAL TECHNOLOGIES

Australia defines critical technologies as current and emerging technologies with the capacity to significantly enhance, or pose risks to, Australia's prosperity, society and national security.

Critical technologies can generate economic and military advantages, particularly for early adopters. This has the potential to significantly alter the balance of power among states. Critical technologies provide new ways for states to pursue their geopolitical interests, with the potential to challenge the international rules-based order. Some states are increasingly conducting coercive grey zone activities in cyberspace, below the threshold of the use of force, to achieve their strategic goals.

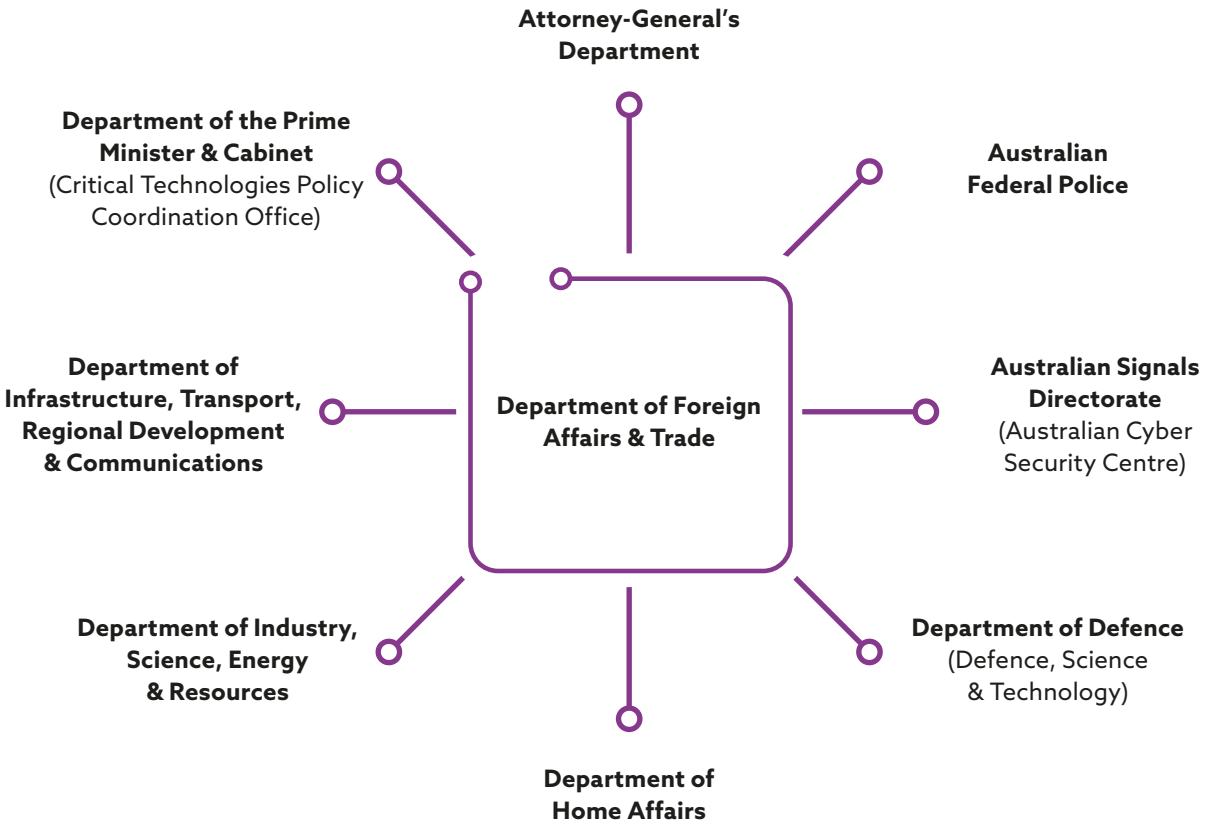
States acting maliciously in cyberspace or by using critical technology increases the risk of international instability. Depending on the circumstances, this may also amount to a breach of international law or an act inconsistent with agreed norms. This challenges countries seeking to use cyberspace and critical technology to promote global prosperity and sustainable development.

Strategic and coordinated national approach to our international engagement

To navigate these challenges we will enhance our cyber and critical technology-related international engagement using a coordinated whole of-Government (WoG) approach. Australia's cyber and critical technology international engagement is coordinated across Government by Australia's Ambassador for Cyber Affairs and Critical Technology within the Department of Foreign Affairs and Trade (DFAT).

The Ambassador for Cyber Affairs and Critical Technology will chair a quarterly WoG International Cyber and Critical Technology Engagement Group (Figure 2) bringing together key Government representatives with responsibility for pursuing Australia's international cyber and critical technology agenda. The Group will work to maximise opportunities to promote Australia's cyber and critical technology interests and objectives internationally.

Figure 2: International Cyber and Critical Technology Engagement Group



We will also seek opportunities to build our capability within our diplomatic network. Those who represent Australia require an in-depth understanding, where needed, of our national interests across cyber and critical technology issues.

Since 2017 we have implemented a Cyber Affairs Curriculum for our Diplomatic Academy to ensure representatives from across Government have a detailed understanding of Australia's cyber affairs agenda. We will expand this curriculum to include critical technology issues.

Prioritising and enhancing our international engagement

Australia will continue to engage with all international partners to promote our cyber and critical technology diplomacy objectives, focusing on the Indo-Pacific region. We will build new and strengthen existing partnerships to help pursue our interests in, and access to, safe, reliable, inclusive and cost-effective critical technologies.

We will strengthen engagement with like-minded democracies to pursue our collective interests and values. These efforts are needed to ensure that cyberspace and the supply and use of critical technologies do not endanger international peace and security and democratic values. Not all countries share these values, and there are diverse perspectives on how to manage the opportunities and risks of cyberspace and critical technology. We will continue to engage with all members of the international community to pursue our national interests.

Harnessing the opportunities of cyberspace and critical technology in the Indo-Pacific is crucial for economic growth, security, and the stability of the region. We recognise the opportunity provided by cyberspace and critical technology to help achieve the Sustainable Development Goals (SDGs) in the Indo-Pacific, and reaffirm our commitment to deliver on the United Nations 2030 Agenda for Sustainable Development.

To reflect the expanded scope of the Strategy, our Cyber Cooperation Program will become the Cyber and Critical Technology Cooperation Program. Through the program, Australia will continue to work with our Indo-Pacific partners to build the capacity needed to harness the opportunities of cyberspace and critical technology while mitigating the risks.

We will coordinate with other donors in the region to ensure coherent development programming that maximises impact and sustainability. This includes through our Cyber Policy Dialogues and key regional and multilateral forums, such as the East Asia Summit, the ASEAN Regional Forum and the Pacific Islands Forum, where we work with partners to coordinate, prioritise and complement cyber and critical technology capacity building.

AUSTRALIA-INDIA FRAMEWORK ARRANGEMENT ON CYBER AND CYBER-ENABLED CRITICAL TECHNOLOGIES COOPERATION

As part of the Australia-India Leaders' Virtual Summit held in June 2020, Australia and India concluded the Australia-India Framework Arrangement on Cyber and Cyber Enabled Critical Technologies Cooperation. Under the Arrangement, Australia and India will work together to promote and preserve an open, free, safe and secure Internet, enhance digital trade, harness critical technology opportunities and address cyber security challenges. The Arrangement will be complemented by a new four-year, $12.7 million Australia-India Cyber and Critical Technology Partnership, creating a research and development fund for Indian and Australian businesses and researchers and to support other countries to improve their cyber resilience. These measures will help shape a global technology environment that meets our shared vision of an open, free, rules-based Indo-Pacific region.

We will enhance our engagement with industry and civil society on cyberspace and critical technology issues, recognising the importance of industry in the design, development and use of critical technologies. Engaging with civil society, academia, and the technical community will help assure new technologies are safer, more transparent, inclusive and explainable.

To promote research and strengthen understanding of cyber and critical technology issues, Australia established the Quad Tech Network (QTN) in 2020. The QTN funds public-facing, policy-relevant research from think-tanks and academic institutions in Quad countries (Australia, Japan, India and the United States). We will continue to engage with the research community to strengthen understanding of cyber and critical technology issues.

By prioritising our cyber and critical technology diplomacy, we will position Australia as an active, trusted and influential leader that shapes international approaches on cyber and critical technology. Australia will actively shape the design, development and use of critical technology in line with our liberal democratic values and interests in a safe, secure and prosperous world.

CYBER AND TECH RETREAT

The Department of Foreign Affairs and Trade and the Office of Denmark's Tech Ambassador have established an annual Cyber and Tech Retreat – a closed multi-stakeholder forum for candid and constructive discussions on technology and foreign policy issues.

Jointly chaired by Australia's Ambassador for Cyber Affairs and Critical Technology and Denmark's Tech Ambassador, the Cyber and Tech Retreat brings together governments, technology companies and academics to explore the increasingly profound impact of critical technologies on the foreign and security policy landscape.

The inaugural retreat was held in San Francisco and Silicon Valley in 2019 with a range of delegates including senior cyber and technology officials from 21 countries, senior executives of US-based technology companies and leading academics. Through frank and open discussion in a private setting, consideration was given to a range of issues arising from the intersection of emerging technologies and international relations. These discussions continued virtually in 2020, due to the travel restrictions of COVID-19.

> I really think that this kind of gathering and the advance of Techplomacy is fundamental to the future. If we're going to better protect technology, if we're going to better protect people who rely on technology, it requires that governments come together in these new ways, it requires that governments interact with the tech sector in new ways. Meetings like this are not only welcome, I think we're going to need more of them.
>
> *Brad Smith (President, Microsoft).*

A specialised vehicle for open engagement, the Cyber and Tech Retreat enables the building of meaningful working relationships where governments and industry are free to jointly understand the longer-term risks, opportunities and impacts of emerging technologies, and their impact upon foreign policy interests.

Ultimately, through this novel forum of technology diplomacy, Australia, Denmark, and a multitude of countries and companies continue to work to promote an open, free, secure and prosperous cyberspace.

VALUES

AUSTRALIA'S GOAL:

Technology is used to uphold and protect liberal democratic values

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- Advocate for cyberspace and critical technologies to uphold and protect democratic principles and processes
- Promote and protect human rights online and in the design, development and use of critical technologies
- Support the ethical design, development and use of critical technologies consistent with international law, including human rights
- Advocate for diversity, gender equality and women's empowerment in the design, development and use of cyberspace and critical technology

Australia's international engagement will seek to shape the design, development and use of cyberspace and critical technologies in line with Australian values. These values are not defined by race or religion, but rather a shared commitment to liberal democratic values including political, economic and religious freedom, the rule of law, racial and gender equality, and mutual respect.

Australia is both a principled and a pragmatic country. While we do not seek to impose our values on others, we believe that where cyberspace and critical technologies are used to uphold and protect liberal democratic values and international law, societies are safer, more secure, enable greater economic growth, and encourage innovation. By seeking to shape international approaches to technology, founded on these values and international law, we will realise their full benefits while protecting against the risks of their misuse to the safety, security and prosperity of Australia, our region and the world.

We will oppose the use of cyberspace and critical technology to interfere with or undermine democratic principles and processes. We will support the promotion and protection of human rights online and through the design, development and use of critical technologies. We will promote the use of cyberspace and critical technologies to advance diversity, gender equality and women's empowerment.

We will cooperate with international partners, multilateral institutions, the private sector, the research community and civil society to achieve these goals.

DEMOCRATIC PRINCIPLES

Australia will: advocate for cyberspace and critical technologies to uphold and protect democratic principles and processes

Australia will do this by:

Action 4. **Supporting** applications of cyberspace and critical technologies that uphold and protect democratic principles and processes

Action 5. **Opposing** the use of cyberspace and critical technologies to interfere, undermine or otherwise weaken democratic principles and processes

All Australian Government policies must give expression to, and be shaped by, Australian community values. While we do not seek to impose our values on others, we are determined to protect liberal institutions and advocate for universal values, human rights and democratic principles and processes. Societies that observe these values will be fairer and more stable. Their economies will benefit as individual creativity is encouraged and innovation rewarded.

Our democracy is defined by the values of the rule of law, freedom of elections and being elected; freedom of assembly and political participation; freedom of expression, religion or belief; and other human rights.

The rule of law, freedom, an independent media, an impartial and independent judicial system and a market economy constitute the fabric of Australian democracy. They support our national strength and high-income economy, providing an enduring basis for social and economic progress. We are committed to protecting our democracy and to using the advantages it bestows on our country to deliver opportunity and security for all Australians.

Cyberspace and critical technologies can strengthen democracy

Cyberspace and critical technologies offer new and enriched ways for governments and people all over the world to uphold democratic principles and actively engage in democratic processes. They provide new ways to share political information online, engage in political movements and campaigns, and to fulfil human rights and freedoms of political participation, opinion and expression. A free and open media is vital to realising these benefits, and to strong and robust democratic processes and governance.

Cyberspace and critical technologies can enhance engagement in democratic processes and promote democratic principles by opening new avenues for governments and political parties to more meaningfully connect with their citizens. This has immense potential for citizens and governments all over the world to build more inclusive, engaged and representative societies.

Australia will support and encourage the use of cyberspace and critical technologies to strengthen and protect democratic principles, processes and other associated freedoms around the world. We will continue to promote this in our bilateral, regional and multilateral engagement and capacity building activities. Australia will also engage with industry and civil society to strengthen mutual understanding of how cyberspace and critical technology can strengthen and reinforce democratic principles and processes.

Cyberspace and critical technologies can undermine and weaken democracy

Australia recognises that cyberspace and critical technologies can also pose significant challenges to democracy. By design, some technologies strengthen censorship, enabling oppression and mass surveillance. The application of technologies in these ways can be used to suppress populations, infringe on political and social rights and deny participation in legitimate political processes.

Democratic societies are also increasingly vulnerable to interference and manipulation by malicious actors. Tolerance, respect, negotiation and social cohesion comprise the basic features of a functioning democracy. Trust is foundational to these features, and malicious actors are increasingly targeting social trust in democratic processes and institutions. Malicious actors may take advantage of and exploit the strengths of democracies, such as a free and open media, to deliberately interfere with democratic processes and undermine trust in pursuit of their geopolitical interests. This may include disrupting electoral processes, targeting voter information, political parties, voting technologies and the reporting of results through the use of cyber or critical technology-enabled means. In some circumstances, this may amount to a breach of international law.

The use of cyberspace and critical technology to undermine, disrupt or distort democratic principles and processes is of great concern to Australia, as it is to all other liberal democracies around the world. Australia will oppose actions that interfere, weaken or erode trust in democratic institutions or processes. This includes cyber and critical technology-enabled foreign interference. Australia will continue our international engagement with regional partners to enhance their resilience, and build support for stronger international action against cyber and critical technology-enabled foreign interference in democratic processes and institutions. This will complement other actions that Australia will take to counter digital disinformation (see Disinformation and Misinformation on page 44), and promote and protect human rights (see Human Rights on page 22).

HUMAN RIGHTS

Australia will: promote and protect human rights online and in the design, development and use of critical technologies

Australia will do this by:

Action 6. **Promoting**, protecting and upholding human rights online and in the design, development and use of critical technologies

Action 7. **Opposing** and condemning the use of cyberspace and critical technologies in a manner that violates human rights and freedoms

Action 8. **Strengthening** the capacity of states to meet their human rights obligations, and of other stakeholders to meet human rights responsibilities online and in the design, development and use of critical technologies

Cyberspace and critical technologies provide new ways to protect and exercise human rights and freedoms. Yet like all technological advances, access to cyberspace and critical technologies can bring benefits or pose risks to the protection of human rights.

Australia has a long-standing commitment to uphold and promote human rights. This is an underlying principle of our international engagement. Australia is committed to upholding and defending the international rules-based order online, including international human rights law, just as we do offline.

Access to cyberspace and critical technologies provides new and increased opportunities for the exercise of the freedoms of expression, peaceful assembly and association, and the promotion and protection of other human rights. Cyberspace and critical technologies enhance participation in democratic processes and provide a unique platform to raise awareness of human rights issues, enabling human rights defenders to better engage with vulnerable communities, as well as amplifying their voice to carry out their work.

Cyberspace and critical technologies create opportunities and risks for human rights

When appropriately designed, technologies such as Artificial Intelligence (AI) and machine learning systems can reduce discrimination through the removal of unconscious bias in decision-making; and help realise the right to equality before the law and access to justice. They can also help realise the right to the highest attainable standards of physical and mental health by improving diagnostics, personalising medical treatment and preventing disease.

Cyberspace and critical technologies can support decision-making in the use of force in domestic law enforcement and in a military context. Such technologies have the potential to support greater compliance with relevant international legal frameworks, as discussed in Annex B.

While cyberspace and critical technologies offer unparalleled opportunities to exercise, promote and protect human rights and freedoms, they can also be used to violate or undermine these rights. Decision-making bias can be built into AI algorithms and data sets, embedding discrimination or decreasing consideration of diversity on the basis of gender, sexual orientation, race, ethnicity, geography, Indigeneity or disability. It requires the active participation of all stakeholders – states, industry, civil society, and the research community – to prevent this.

The use of cyberspace and critical technologies inconsistent with international human rights law is of great concern to Australia. Many countries around the world increasingly use cyberspace and critical technologies to violate individuals' human rights and freedoms and prevent participation in democratic processes. This has included targeted hacking, mass online surveillance, the collection of personal and biometric information, the arrest and intimidation of online activists, the identification, profiling and restriction of members of particular cultural, religious or political groups, or through the use of facial recognition and other surveillance technology to monitor the everyday activities of individuals in a manner inconsistent with international human rights law.

Some countries are increasingly using cyberspace and critical technologies to pursue arbitrary or unlawful politically motivated content censorship, including through the deliberate use of Internet 'shut downs'. This is often done under the pretext of national security. The international community, including Australia, recognises the legitimate security needs and concerns of states and that limitations on some human rights and freedoms are permitted under particular circumstances. However, all countries have a duty to ensure these limitations are consistent with their obligations under international human rights law.

Supporting human rights is an underlying principle of Australia's foreign policy and international engagement. Australia is a member of the Freedom Online Coalition, and supports capacity building in ASEAN and the Pacific through Australia's Cyber and Critical Technology Cooperation Program to strengthen human rights and promote democratic principles online.

Promoting, protecting and upholding human rights

Australia considers that individuals should enjoy human rights and freedoms online just as they do offline, including the design, development and use of critical technologies. We will advocate for the use of cyber and critical technologies to strengthen the promotion and protection of human rights and freedoms through continued engagement in multilateral and regional forums, and will raise human rights concerns and highlight opportunities in our bilateral engagement.

Oppose and condemn violations of human rights and freedoms

Australia condemns all attempts to violate human rights or freedoms using cyberspace or critical technology-enabled means. The use of Internet shutdowns to limit freedom of expression, freedom of assembly and involvement in democratic processes is of particular concern. Australia may publicly call out states, including through the Human Rights Council's Periodic Review Process, that deliberately or systematically use Internet shutdowns to stifle legitimate and peaceful opposition, and prevent people from voting or participating in democratic processes. For example, through the UN Human Rights Council, Australia has urged Myanmar to lift media and Internet restrictions in the Rakhine and Chin states.

INTERNET SHUTDOWNS

Australia is concerned by the trend of increasingly deliberate use of unlawful Internet shutdowns, including severe restrictions and blocking of certain content, in many parts of the world. According to civil society group Access Now, 1,706 days of Internet access were disrupted by 213 Internet shutdowns across 33 countries in 2019. They found that Internet shutdowns were increasing in number, lasting longer, affecting more people and targeting vulnerable groups.

Internet shutdowns are often prosecuted under the guise of national security, public safety, or to stop the spread of disinformation online. In reality, they are more likely to be politically motivated, and in some circumstances amount to an unlawful limitation of rights, such as the freedom of expression and freedom of assembly.

The international community, including Australia, recognises the legitimate security needs and concerns of states and that some limitations on human rights and freedoms are permitted under certain circumstances. However, all countries have a duty to ensure these limitations are consistent with their obligations under international human rights law.

Strengthening the capacity of states and other stakeholders

Australia will support capacity building in the Indo-Pacific to strengthen regional capacity to uphold and protect human rights online and through the design, development and use of critical technologies. A key focus of Australia's Cyber and Critical Technology Cooperation Program is to strengthen stakeholders' understanding of how to protect human rights online. Through the program, we support activities across the region that increase partner capacity to respond to and manage issues in a manner consistent with human rights online and through the design, development and use of critical technology.

This includes ongoing engagement with, and support of, non-government organisations (NGOs), civil society and industry groups. We will increase awareness and capacity for industry to meet its responsibility to respect human rights, in line with the *UN General Assembly Third Committee resolution on the right to privacy in the digital age and the UN Guiding Principles on Business and Human Rights*.

ETHICS OF CRITICAL TECHNOLOGY

Australia will: support the ethical design, development and use of critical technologies consistent with international law, including human rights

Australia will do this by:

Action 9. **Engaging** in multilateral forums and processes to shape global ethical principles and frameworks on critical technologies

Action 10. **Sharing** best practice approaches to the ethical design, development and use of critical technologies, consistent with international law including human rights

Action 11. **Working** with industry, civil society and the research community to develop non-binding ethical frameworks for critical technologies consistent with human rights

Incorporating ethical, human rights-based approaches into the design, development and use of critical technology can help ensure they benefit societies around the world. The world is at an inflection point, and cooperation is vital to ensure non-binding ethical frameworks that align with international law, including human rights, are considered in the design, development and use of critical technologies.

The world is on the precipice of a new era of technological disruption, which will transform our societies, ways of living, and our safety and wellbeing.

With these opportunities come challenges. The proliferation of intelligent, autonomous systems may pose difficult questions about how decisions are made and why. The growth in the collection, analysis and use of personal and biometric data involves significant and complicated considerations of convenience, functionality, rights and freedoms that are not always readily apparent. Some advances in Artificial Intelligence (AI), bioengineering and neuro technology even raise fundamental questions about what it means to be human, as technologies assume attributes or alter functions that were previously considered uniquely human. Some technologies may also be used in ways different to the original intent, increasing the complexity of how we respond.

Ethical frameworks that are consistent with international law including human rights

In response to these challenges, many stakeholders are looking to establish ethical frameworks to guide how technologies are designed, developed and used. These non-binding ethical frameworks can help ensure technologies are used to benefit people and societies, while mitigating potential risks from their use or deliberate misuse.

Australia believes existing international law, including international human rights law, must be the foundation for the ethical design, development and use of critical technologies. International human rights law has been developed from fundamental, universal principles on the value and dignity of human life. In addition to international human rights law, initiatives such as the United Nations (UN) *Guiding Principles on Business and Human Rights* provide a global standard and guidance to the private sector on how they can prevent and address the risk of adverse human rights impacts linked to business activity. Existing international law and principles therefore provide the most suitable basis on which to develop non binding ethical principles and frameworks for critical technologies.

Australia opposes the development of new non-binding ethical principles or frameworks that are not consistent with existing international law, including human rights. This risks creating confusion, inconsistency and lack of clarity regarding states' existing obligations under international law.

GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE

Australia is a founding member of the Global Partnership on AI (GPAI). GPAI is an international and multi-stakeholder initiative to guide the responsible development and use of AI, grounded in human rights, inclusion, diversity, innovation and economic growth. The initiative is the first of its kind.

GPAI will support the responsible and human-centric development and use of AI in a manner consistent with human rights, fundamental freedoms, and shared democratic values, as elaborated in the Organisation for Economic Cooperation and Development (OECD) Council *Recommendation on AI*.

Founding members include Australia, Canada, the European Union, Germany, India, France, Italy, Japan, New Zealand, the Republic of Korea, Singapore, Slovenia, the United Kingdom and the United States.

Engagement and capacity building on ethical frameworks

Australia will continue to engage in multilateral forums, processes and with cross-regional groups to shape the development and share best practice approaches to the establishment of ethical frameworks that are consistent with international law and human rights, such as Australia's AI Ethics Framework. This includes working with countries in our region through our Cyber and Critical Technology Cooperation Program, to promote the ethical design, development and use of critical technologies. Australia recognises the essential role of industry and civil society to shape and develop ethical frameworks on critical technologies, and commits to strengthening our engagement and collaboration with them to achieve this goal.

AUSTRALIA'S AI ETHICS FRAMEWORK

The Australian Government's Department of Industry, Science, Energy and Resources AI Ethics Framework was released in November 2019 to help guide businesses and governments seeking to design, develop, deploy and operate AI in Australia.

The principles are aspirational and intended to provide organisations with a signpost as to how AI should be developed and used in Australia. The eight principles (see below) are voluntary and intended to complement existing AI-related regulations. These ethics principles build on the human rights framework.

1. Human, social and environmental wellbeing
2. Human-centred values
3. Fairness
4. Privacy protection and security
5. Reliability and safety
6. Transparency and explainability
7. Contestability
8. Accountability

We are working across government, industry and academia to ensure Australia's AI ethics principles are implemented effectively.

DIVERSITY & GENDER EQUALITY

Australia will: advocate for diversity, gender equality and women's empowerment, in the design, development and use of cyberspace and critical technology

Australia will do this by:

Action 12. **Promoting** greater diversity and inclusiveness in the design, development and use of cyberspace and critical technology

Action 13. **Advocating** for gender equality and women's empowerment, and supporting greater awareness of the effect of cyberspace and critical technologies on gender equality

Action 14. **Embedding** gender sensitivity and the meaningful inclusion and leadership by women and girls as key principles in Australia's cyber and critical technology capacity building

To maximise the benefits of cyberspace and critical technology, and build inclusive, safe and more prosperous societies, it is crucial that all stakeholders are included and empowered. This includes: promoting greater diversity, gender equality and women's meaningful participation and leadership in cyberspace and critical technology policy-making, implementation and representation; the design and development of critical technology; and, the broader cyber and critical technology workforce. It also includes raising awareness of the impact cyberspace and critical technology can have on groups at risk of discrimination and exploitation, such as women and girls.

Our societies are fairer, safer and more prosperous when we remove barriers to inclusion and ensure all individuals – regardless of gender, race, ethnicity, religion, socio-economic background, sexual orientation or ability – contribute to, and are considered across all aspects of cyberspace and critical technology.

Promoting diversity

Australia's international engagement on diversity and gender equality goes beyond our international human rights obligations, to consider how we can promote greater diversity and inclusiveness in cyberspace and critical technology to maximise the benefits across society.

We recognise the lack of diversity in those who design and develop technologies; those responsible for setting, implementing, regulating and representing policy; those who make decisions; and, those who have access to technologies.

We also recognise the different impacts this lack of diversity in cyber and critical technology has on end users, particularly those at risk of discrimination. For example, children, women, LGBTI+ persons, persons with disabilities, Indigenous people, and racial and ethnic minorities are under-represented and particularly vulnerable to discrimination. These groups of people, particularly those at the intersections of different forms of vulnerability, often experience greater online harms and negative experiences.

Australia, through our multilateral, bilateral and regional engagement, will advocate for greater diversity and inclusiveness in cyberspace and critical technology, and will work with industry and civil society partners to promote these objectives.

WOMEN IN INTERNATIONAL SECURITY AND CYBERSPACE FELLOWSHIP

Australia, together with Canada, The Netherlands, New Zealand and the United Kingdom, launched the *Women in International Security and Cyberspace Fellowship* in February 2020. The Fellowship provides early-to mid-career female diplomats from all over the world with training on multilateral negotiations, cyber policy and international law, and sponsors their attendance at UN meetings that consider responsible state behaviour in cyberspace.

CYBER SAFETY FOR PACIFIC WOMEN

The Department of Foreign Affairs and Trade is supporting the Australia Pacific Security College, in partnership with UN Women, to develop a range of cyber safety training materials for women and girls. This aims to provide them with the necessary skills to realise the considerable opportunities, and mitigate the risks, presented by increased digital access.

Gender equality and women's empowerment

Of particular concern and interest to Australia is the impact of cyberspace and critical technology on gender equality and women's empowerment.

Gender inequality undermines global prosperity, stability and security. It contributes to, and often exacerbates, a range of challenges, including poverty, weak governance, conflict and violent extremism. The value of gender equality and women's empowerment is indisputable. Women's participation in decision-making, leadership and peace building is important as it brings particular perspectives, priorities and strengths, which are often different from men's. Women's economic participation helps to drive growth at a national level and reduce poverty within communities and households such that societies that better leverage the skills, talents, perspectives and time of everyone will be more likely to prosper.

The International Telecommunication Union (ITU) estimates that only 48.4 per cent of the total global female population is using the Internet, compared to 58.2 per cent of all men – a digital gender gap of 9.8 per cent. While the world continues to enjoy the significant benefits of increased Internet accessibility, systemic economic and societal barriers mean that its dividends are less likely to flow to women. Moreover, women are less likely to have reliable access to mobile financial services than men, and face difficulties controlling their own digital identities and health records. Women are also significantly under-represented in international discussions on security and responsible state behaviour in cyberspace.

UNITED NATIONS (UN) WOMEN: *INNOVATION FOR GENDER EQUALITY*

UN Women is the UN organisation dedicated to gender equality and the empowerment of women. A global champion for women and girls, UN Women was established to accelerate progress on meeting their needs worldwide. Its 2019 report *Innovation for Gender Equality* noted that

> ...it is increasingly clear that technology and innovation can be rejected; that they can create new, unforeseen problems of their own; and that they do not benefit all equally. Not only are women under-represented across core innovation sectors, including science, technology, engineering and mathematics (STEM), but new technology brings risks of bias and possibilities for misuse, creating new human rights challenges for the 21st century.

Recognising this, the Australian Government's *Advancing Women in STEM* Strategy, led by our Women in STEM Ambassador, is focused on providing leadership and driving efforts to: support the active inclusion of girls and women in STEM education (from early education to tertiary); promote workplaces that support the active recruitment and retention of women in STEM roles at all levels; and, ensure girls and women see STEM education and professions as viable and interesting career paths.

Australia's international engagement on cyberspace and critical technology issues aims to complement and further the work of our Ambassador for Gender Equality. It will ensure that gender equality, the empowerment of women and girls, our commitments under the Women, Peace and Security agenda and efforts under Sustainable Development Goal 5 are a central focus of our diplomatic, development and regional security efforts. Gender equality and women's empowerment is integrated throughout the Cyber and Critical Technology Cooperation Program, including at all stages of the project management cycle. The program sets aside five per cent of its total funding to ensure gender equality is adequately considered throughout implementation and to support stand alone gender equality initiatives.

We also continue to support mainstreaming gender equality and parity within the UN, including through the *UN System-wide Action Plan (UN-SWAP) on Gender Equality and the Empowerment of Women,* and the ITU *Gender Equality and Mainstreaming Policy*.

Critical technology can perpetuate discrimination against women

Technology reflects the society in which it is designed, developed and used. Where gender inequality and discrimination against women and girls exists, so too will inequality exist in access and use of cyberspace and critical technologies.

Violence against women and girls, which is increasingly prevalent online, is a significant human rights violation that causes harm by limiting women's social, political and economic participation. This includes behaviours such as abusers using tracking apps, monitoring Internet search history, restricting access to passwords or account settings, or inflicting economic or emotional abuse.

Given the central role that critical technologies increasingly play in all facets of life, women's under-representation in the design, development and use of critical technologies is of considerable concern. Gender bias is likely where data sets used for training AI algorithms are not representative of women and girls. Meaningful participation, leadership and representation of women throughout these processes, and the technology sector more broadly, are therefore critical to ensuring the production of technologies that meet the needs of our society as a whole.

Through our international engagement, Australia will advocate to empower women and girls to stay safe online. We will continue to advocate for the creation and implementation of frameworks, standards and principles such as, the Organisation for Economic Cooperation and Development (OECD) *Recommendations on AI*, the G20 *AI Principles* and eSafety's *Safety by Design* initiative, that meaningfully address critical technology gender issues, such as inclusivity and safety. We will also work with partners in the technology industry to advocate for gender equality at all stages of the technology lifecycle.

ESAFETY WOMEN

eSafety Women provides practical tools and information to equip all women to protect themselves and their families against all forms of technology-facilitated abuse, including image-based abuse.

During the COVID-19 pandemic, eSafety leveraged these resources to develop a COVID-19 Global online safety guide for frontline workers supporting women. This resource was distributed to over 60 multilateral organisations and disseminated globally in partnership with the Department of Foreign Affairs and Trade.

eSafety will continue to make these resources available to women globally, with a focus on the Indo-Pacific region, as part of its work funded under the Cyber and Critical Technology Cooperation Program.

SECURITY

AUSTRALIA'S GOAL:

Secure, resilient
and trusted technology

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- Shape the development and use of critical technology, including cyberspace, to support international peace and stability
- Build international resilience to digital disinformation and misinformation and their effects
- Build a strong and resilient cyber security capability for Australia, the Indo-Pacific and the world
- Strengthen cooperation for enhanced prevention, detection, investigation and prosecution of cybercrime
- Enable a safe and inclusive online environment

The malicious use of cyberspace and critical technologies poses clear risks to the security and safety of Australians, our country, the Indo-Pacific region and the world. We will take action to strengthen our capability, and that of our region, to manage and respond to threats to security and safety enabled by cyberspace and critical technologies.

The value of international partnerships in responding to cyber threats and cybercrime has been demonstrated through our experience in responding to these risks. We will continue to strengthen our partnerships on cyber security and cybercrime prevention, detection and prosecution to help guard Australia and our region from these threats. New means of political and economic coercion are enabled by unlawful invasive surveillance, and disinformation is enhanced by the capabilities of cyberspace and critical technologies. We will expand our engagement with partners to increase capability to identify and effectively manage technology-enabled threats, such as disinformation.

This work is underpinned by our advocacy for responsible state behaviour in cyberspace, founded in the application of existing international law and agreed norms of behaviour. Australia's position is that states must comply with their obligations under international law, including the UN Charter, when using technologies, and encourage states to make use of the established international legal framework that supports international cooperation to combat cybercrime.

Only by taking action to mitigate the risks born of the malicious misuse of technology can we realise the full range of benefits they offer.

INTERNATIONAL PEACE & STABILITY

Australia will: shape the development and use of critical technology, including cyberspace, to support international peace and stability

Australia will do this by

Action 15. **Setting** clear expectations for responsible state behaviour

Action 16. **Deterring** malicious activity enabled by critical technologies, including cyberspace, and responding when it is in our national interests

Action 17. **Cooperating** with other states to hold to account those that engage in unacceptable behaviour

Action 18. **Implementing** practical confidence building measures to promote international peace and stability and prevent conflict

Critical technologies, including cyberspace, have had, and continue to have, a positive impact on international peace and stability. However, the ways in which critical technologies may be used to undermine international peace and stability are proliferating. International cooperation is vital to ensure critical technologies continue to support a peaceful and stable international environment.

Since the release of the 2017 *International Cyber Engagement Strategy,* states have continued to pursue activities in cyberspace that challenge the rules-based international order. We are seeing similar behaviour with critical technologies as states compete for strategic dominance in an increasingly competitive international environment.

The risks of malicious misuse of technologies can contribute to increasing strategic instability that, if unchecked, increases the risk of misperceptions and miscalculations between states that might escalate to conflict. Australia's focus in maintaining international peace and stability is on the use (or misuse) of critical technologies, rather than regulating the technologies themselves. Our endeavours in this regard recognise and consider the gender dimensions that underpin international peace and security.

THE UNITED NATIONS (UN) FRAMEWORK FOR RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

All members of the UN have agreed, by consensus, that existing international law – in particular, the Charter of the UN in its entirety – is applicable in cyberspace and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment [see UNGA resolutions A/RES/68/243; A/RES/70/237]. All states have also endorsed 11 voluntary non binding norms of responsible state behaviour, and recognised the need for confidence building measures (CBMs) and coordinated capacity building. Combined, these measures (international law, norms, CBMs and capacity building) provide the basis for a secure, stable and prosperous cyberspace, and are often referred to as the UN Framework for Responsible State Behaviour (the Framework). Each element of the Framework is mutually reinforcing and no one element should be considered in isolation.

Universal endorsement of the Framework for Responsible State Behaviour in Cyberspace represents good progress towards promoting international peace and stability in cyberspace; states should consider the structure of this Framework when agreeing on responsible states' use of critical technologies. If adhered to, existing international law, complemented by voluntary norms of responsible state behaviour, CBMs and capacity building, provides a robust framework to address the threats posed by state-generated and state-sponsored malicious cyber activity.

The priority now is deepening understanding and practical implementation of this Framework, and ensuring accountability when states disregard their obligations and responsibilities.

WOMEN, PEACE AND SECURITY

As a global leader on the Women, Peace and Security (WPS) agenda, Australia strongly advocates for the meaningful participation of women in all stages of conflict prevention, crisis management and peacebuilding, bringing their unique experiences of conflict and crises to promote stability, social cohesion and sustainable peace.

Responsible state behaviour

INTERNATIONAL LAW

Existing international law is applicable to state conduct in cyberspace – the focus of the international community is now on articulating *how* it applies.

Australia has articulated its views on how particular principles of international law apply to state conduct in cyberspace (2017; 2019) and published hypothetical legal case studies (2020) (Annex A to this Strategy combines those previously published positions). This forms part of Australia's efforts to publish our views on how international law applies to state conduct in cyberspace. To foster common understandings, we urge all countries to do the same; developing and articulating national positions on existing international law will equip states to exchange views and deepen common understandings of how existing international law applies in cyberspace.

Just as existing international law applies to cyberspace, existing international law – including the UN Charter in its entirety – applies to the design, development and use of critical technologies by states. Australia is committed to working with international partners, and with industry, civil society and the research community, to strengthen understanding of how international law applies to the development and use of critical technologies.

Australia is committed to supporting countries to develop national positions on how international law applies to the design, development and use of critical technologies as necessary, as well as to state conduct in cyberspace.

> Australia reaffirms our commitment to act in accordance with the recommendations of UN Group of Governmental Experts, as endorsed by the General Assembly, and we call on all countries to do the same.
>
> *Dr Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology, address to the UN Security Council Arria-Formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building, May 2020.*

NORMS OF RESPONSIBLE STATE BEHAVIOUR

International law does not stand alone. Recognising the unique attributes of cyberspace, in 2015 all states agreed to be guided in their use of ICTs by eleven voluntary and non-binding norms of responsible state behaviour in cyberspace. These norms complement, but do not replace states' existing legal obligations. Combined, they establish clear expectations of responsible behaviour. By signalling acceptable behaviour for states, international law and norms promote predictability, stability and security.

To be effective, the eleven agreed norms must be implemented by all countries. Practical guidance supported by coordinated capacity building, is needed so that all countries are in a position to implement the agreed norms. In support of this, Australia has

published non-exhaustive examples of the ways in which Australia observes the eleven norms.

Australia – through our Cyber and Critical Technology Cooperation Program – will continue to support targeted capacity building to ensure that ASEAN and Pacific Island countries are able to respond to the challenges and embrace the opportunities that cyberspace and critical technologies provide. This includes: providing assistance to help countries identify and fill gaps in norm implementation, or to support active engagement in discussions on the articulation of norms in relation to critical technology; and supporting countries to implement CBMs.

UN GROUP OF GOVERNMENTAL EXPERTS AND UN OPEN ENDED WORKING GROUP

Australia is actively involved in two UN processes discussing responsible state behaviour in cyberspace – a sixth Group of Governmental Experts (GGE) [A/RES/73/266] and an inaugural Open Ended Working Group (OEWG) [A/RES/73/27]. Previous iterations of the GGE developed the Framework of Responsible State Behaviour in Cyberspace, which has been endorsed by all countries, by consensus, at the United Nations General Assembly. Australia's priorities for both this GGE and the OEWG are: to deepen understandings of how existing international law and agreed norms apply; agree practical guidance on how to implement the recommendations of previous GGE reports; and, develop recommendations to better coordinate and target cyber capacity building in support of implementation. We will continue to actively engage in these processes and any future iterations of multilateral discussions of responsible state behaviour in cyberspace.

As technology becomes increasingly critical to our way of life, consideration of what is acceptable state conduct will increase in importance. Australia considers that the elements of the Framework of responsible state behaviour in cyberspace could provide a model for articulating acceptable responsible state behaviour for the design, development and use of particular critical technologies. For instance, it may be appropriate, in particular contexts, for states to clarify how existing international law applies to states' use of a particular critical technology, or to consider the value of agreeing complementary voluntary non-binding norms with respect to that technology. Australia will support and shape these discussions in line with our values, national interests, the international rules-based order, and our commitment to maintaining a peaceful and stable international environment.

UN GROUP OF GOVERNMENTAL EXPERTS ON LETHAL AUTONOMOUS WEAPONS SYSTEMS (LAWS)

The open-ended UN Group of Governmental Experts (GGE) process underway within the Convention on Certain Conventional Weapons (CCW) was established in 2016 to examine emerging technologies in the area of lethal autonomous weapons systems (LAWS) in the context of the objectives and purposes of the CCW. This process reflects international recognition that the peace and stability dimensions of incorporating emerging technologies such as Artificial Intelligence and robotics into military capabilities must be considered by the international community. Australia welcomes the affirmation by the GGE on LAWS that international humanitarian law continues to apply fully to all weapons systems, including LAWS. We will continue to support processes that strengthen understandings of the responsible use of specific technologies in the context of international peace and stability.

Deter and respond to unacceptable behaviour

Some state and state-sponsored actors increasingly flout international law and norms, in spite of the clear expectations set by the international community of responsible behaviour in cyberspace. In doing so, they threaten international peace and stability.

Deterring malicious cyber activity protects our national interests, maintains international stability and promotes continued global economic growth. The objective of Australia's cyber deterrence efforts is to prevent cyber activity that is damaging to Australia and detrimental to our interests, including those of our partners.

As responsible states that uphold the international rules-based order, we recognize our role in safeguarding the benefits of a free, open, and secure cyberspace for future generations. When necessary, we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behaviour in cyberspace.

Joint Statement on Responsible State Behaviour in Cyberspace, 23 September 2019

AUSTRALIA'S STATEMENT OF PRINCIPLES ON CYBER DETERRENCE

We work to actively prevent cyber attacks, minimise damage, and respond to malicious cyber activity directed against our national interests. We deny and deter, while balancing the risk of escalation. Our actions are lawful and aligned with the values we seek to uphold and will therefore be proportionate, always contextual and collaborative. We can choose not to respond.

Australia's cyber deterrence posture consists of four core elements.

1. **Denial practices** – Australia will ensure that we can discourage, detect, disrupt and contain malicious cyber behaviour thereby increasing the cost and reducing the benefits for perpetrators.
2. **Signalling** – Australia will provide clear, consistent and credible messages to demonstrate our willingness and ability to impose costs on those who carry out malicious cyber activity.
3. **Responses** – Australia will respond to malicious activity in cyberspace, just as we will to any other malicious activity against Australia's interests. Australia's responses to malicious cyber activity could comprise law enforcement or diplomatic, economic or military measures as appropriate. Australia will only respond when it is in our national interests to do so and responses will not always be public. The objective of responding is to promote responsible state behaviour, thereby protecting a peaceful and stable international environment.
4. **International cooperation** – Australia will work with other states to strengthen global responses to unacceptable behaviour. Our ability to deter and respond to malicious cyber activities is stronger when we act in concert with our allies and partners. International coordination and information sharing on attribution, signalling and responses creates a force multiplier effect.

Australia's responses to malicious cyber activity could comprise law enforcement or diplomatic, economic or military measures as appropriate. Our ability to deter and respond to malicious cyber activity is founded on the strength of our cyber security posture.
The Government's significant investment in this capability ensures Australia can discourage, detect, respond to and contain malicious cyber activity that affects our national security and interests (see Cyber Security on page 48).

Just as we act to deter and respond to malicious activity in cyberspace, so too will we work to prevent other technologies being used to undermine our national security and international peace and stability. Consistent with our established cyber deterrence posture, Australia will similarly develop and define our approach to deterring the irresponsible use of critical technology.

PUBLIC ATTRIBUTIONS BY AUSTRALIA

Public attribution of malicious cyber activities to states is one tool in Australia's toolkit of responses. Since 2017, Australia has worked with international partners and attributed malicious cyber activity to state actors on eight occasions:

- December 2017, Australia attributed the 'WannaCry' ransomware campaign to the Democratic People's Republic of Korea
- February 2018, Australia attributed the 'NotPetya' malware attacks on critical infrastructure and businesses to Russia
- April 2018, Australia attributed the worldwide targeting of Cisco routers to Russian state-sponsored actors
- August 2018, Australia called-out Iran for a spear-phishing campaign against Australian universities. This followed an earlier attribution by the United Kingdom and the United States
- October 2018, Australia attributed a pattern of malicious cyber activities and, separately, cyber operations against OPCW and MH17 investigations to Russia
- December 2018, Australia attributed to China a global campaign of malicious cyber activity targeting Managed Service Providers, including in Australia
- February 2020, Australia attributed to Russia a malicious cyber operation targeting Georgia
- July 2020, Australia attributed to Russian actors malicious cyber activity targeting organisations involved in COVID-19 vaccine development.

Confidence building measures

Australia will continue to develop and implement Confidence Building Measures (CBMs) to reduce the risk of conflict stemming from the malicious use of cyberspace by promoting trust and assurance among states, increasing inter-state cooperation, and promoting transparency, predictability and stability. We will expand this work to incorporate consideration of critical technologies.

This includes transparency measures such as participating in policy dialogues, discussion on the rights and obligations of states in the use of offensive cyber and critical technology capabilities. We will also encourage countries to develop and publish their own cyber and critical technology international engagement strategies.

CONFIDENCE BUILDING MEASURES – PROMOTING TRANSPARENCY ON OFFENSIVE CYBER CAPABILITIES

Australia recognises the legitimate right of countries to develop offensive cyber capabilities. Many countries already have, and more are in the process of developing, these capabilities. Australia is one of a few countries that has publicly declared that we develop and use such capabilities. Australian cyber operations comply with Australian law and are conducted in accordance with international law – including the UN Charter in its entirety – as well as agreed norms of responsible state behaviour.

We recognise that, similar to other military capabilities, details of specific capabilities and operations will need to remain classified. However, Australia is transparent about the existence of our offensive cyber capabilities in order to foster a more mature conversation about the rights and obligations that govern their use, particularly the cumulative reports of the UN GGEs, as endorsed by consensus by the UN General Assembly [A/RES/65/41; A/RES/68/243; A/RES/70/237].

Australia encourages other countries to be similarly transparent about their capabilities and unequivocal in their commitment to act in accordance with the agreed Framework for Responsible State Behaviour – transparency breeds accountability, predictability and stability.

Australia will continue to develop and promote risk reduction measures, to build confidence in states' ability to respond to specific instances of malicious cyber activity without escalation.

We will also continue to engage in cooperative measures, to promote collaboration between countries, based on a mutual commitment to improve resilience and reinforce a peaceful and stable online environment. This includes, for example, information exchange on best practices, such as through our Cyber Bootcamp Project for selected ASEAN and Pacific countries.

ASEAN REGIONAL FORUM POINT-OF-CONTACT DATABASE

Australia and Malaysia's proposal for an ASEAN Regional Forum (ARF) cyber points of contact directory was approved by Ministers in 2020. The directory is a simple, voluntary confidence building measure, consisting of relevant points of contact from participating ARF members. The directory is a foundational risk reduction measure which seeks to facilitate near real time communication in the event of ICT security incidents of potential regional security significance.

DISINFORMATION & MISINFORMATION

Australia will: build international resilience to digital disinformation and misinformation and their effects

Australia will do this by:

Action 19. **Building** international partnerships with governments, industry and civil society to increase awareness of, and enhance resilience to, digital disinformation and misinformation

Disinformation and misinformation can limit the independent decision making of governments and the private sector, affect economic prosperity, damage social cohesion, and undermine national security and sovereignty. We will continue to foster greater collaboration between governments, the technology industry, civil society and the research community to address and respond to these risks.

Australia distinguishes between disinformation and misinformation, and seeks to increase awareness of, and enhance our resilience to, their potential harm.

FOREIGN INTERFERENCE

Australia defines foreign interference as activity conducted by or on behalf of a foreign actor, which is coercive, deceptive, clandestine or corrupting, and is contrary to Australia's sovereignty, values and national interests.

DISINFORMATION

Australia defines disinformation as the intentional creation and dissemination of wholly or partly false and/or manipulated information that is **intended to deceive and mislead** audiences and/or obscure the truth for the purposes of causing strategic, political, economic, social, or personal harm or financial/commercial gain.

MISINFORMATION

Australia defines misinformation as the creation and dissemination of wholly or partly false information, **spread unwittingly, by error or mistake**. Such information has the potential to mislead or deceive but is neither created nor transmitted with the intention of doing so or causing harm.

The increasing ubiquity of cyberspace and social media platforms as a source of information and for personal engagement on a wide range of social and community issues has made them a key venue for the dissemination and amplification of disinformation and misinformation.

Disinformation may be used as a tool for foreign interference. Foreign actors continue to spread disinformation to serve their own strategic interests and to undermine public trust in democratic institutions and confidence in official messaging, disrupt the proper functioning of open media, or undermine social cohesion.

Recent electoral processes around the world have shown that digital disinformation campaigns have low barriers to entry, and that malicious actors have effectively hijacked public discourse to influence communities and broader public opinion on matters of significant importance. Unwittingly, platforms designed to promote openness have been misappropriated to promulgate and amplify disinformation and misinformation, sow division and mistrust, and ultimately pervert public discourse.

Malicious use of critical technologies is increasingly occurring to amplify these campaigns. This includes 'bots' that drown out legitimate online debate, data-driven technologies that enable malicious or harmful micro-targeting of susceptible and/or influential audiences, and machine learning-enabled 'deep fakes' that spread disinformation.

Disinformation should be differentiated from foreign influence. All governments can seek to influence discussions on issues of importance. When conducted in an open and transparent manner, foreign influence can contribute positively to public debate and form a legitimate part of international engagement.

In 2019, Oxford University estimated that 70 countries around the world were involved in organised social media manipulation campaigns. Stanford University has identified 570 deceptive 'news' websites receiving over 70 million monthly engagements on Facebook – a volume comparable to mainstream media outlets. MIT has concluded that false news stories are 70 per cent more likely to be shared on Twitter than true stories, and reach 1,500 people in a sixth of the time.

Building international partnerships

Australia will use our international engagement and public communications resources to promote facts and transparency, underpinned by liberal democratic values. We will continue to work with partners around the world to identify and mitigate these risks, and collaborate with partners in our region to enhance their awareness and strengthen their resilience.

Australia will continue to build awareness and capability in South-East Asia and the Southwest Pacific to manage information interference and misinformation. The Cyber and Critical Technology Cooperation Program will work to strengthen approaches to counter disinformation, including through the delivery of online training, advisory support and knowledge exchange to government officials and civil society.

> Concerningly, we have seen disinformation pushed and promoted around the coronavirus pandemic and around some of the social pressures that have been exacerbated by the pandemic... The disinformation we have seen contributes to a climate of fear and division when, at a time like this, what we need is cooperation and understanding...[In June 2020] Australia co-signed with 131 other countries and observers, a Latvian-led statement in the UN warning that COVID-19 had, and I quote, 'created conditions that enabled the spread of disinformation, fake news and doctored videos to foment violence, to divide communities'. We committed in that statement to fighting the so-called 'infodemic'. I can assure you that Australia will resist and counter efforts of disinformation. We will do so through facts and transparency, underpinned by liberal, democratic values that we will continue to promote at home and abroad...
>
> *Australia and the world in the time of COVID-19: Foreign Minister's Speech, National Security College, Australian National University, 16 June 2020*

Australia recognises the active and indispensable role played by industry, and in particular social media companies, in identifying and countering digital disinformation and misinformation. We will continue to foster greater collaboration between governments, the technology industry, civil society and the research community to address and respond to these challenges. We will work with industry to promote the design, development and use of critical technologies that provide communities with safer, informed and transparent access to diverse information. Where cooperation is not forthcoming, other policy and regulatory responses will be considered.

Protecting freedom of expression is an underlying principle of Australia's foreign policy. We are alert to the risk that some states may seek to characterise legitimate debate and commentary that is objectionable to them as disinformation or misinformation. We will continue to advocate for the creation of rules and partnerships that encourage information transparency and enable the identification and mitigation of disinformation and misinformation, whilst respecting the right to freedom of expression.

AUSTRALIAN ELECTORAL COMMISSION'S *STOP AND CONSIDER* CAMPAIGN

The Australian Electoral Commission's (AEC) *Stop and Consider* campaign was launched in the lead up to the 2019 federal election. This social media campaign was the first of its kind run by the AEC and encouraged voters to check the source of electoral communication they saw, heard or read to avoid being misled by misinformation. The AEC recognised the significant interest in the effect of electoral misinformation and disinformation on the continued trust in the integrity of the federal election process and results.

CYBER SECURITY

Australia will: build a strong and resilient cyber security capability for Australia, the Indo-Pacific and the world

Australia will do this by:

Action 20. **Partnering** in our region to strengthen collective cyber security and incident response capabilities

The scale and sophistication of cyber threats to Australia and the Indo-Pacific is increasing. In Australia, it is estimated that malicious cyber activity targeting businesses costs the economy up to $29 billion annually. The way we create, use, store and transmit information is changing, producing new vulnerabilities. Critical technologies will inevitably create new means and methods for actors to conduct malicious cyber activity, while also assisting efforts to defend against these threats.

Australia cannot, and does not, act in isolation in addressing cyber threats. International partnerships create opportunities for information sharing, operational collaboration and support, and cooperation to build technical capacity.

Enhancing the cyber security of Australia enhances that of our region. Australia's security, and those of our partners, benefit from growth in our collective cyber security capacity. As the Indo-Pacific's dependency on cyberspace grows, protecting the confidentiality, integrity and availability of critical networks and infrastructure is vital to ensuring the region is characterised by political independence, inclusive economic growth, stability, security and resilient societies.

Through the *Cyber Security Strategy 2020*, Australia is investing $1.67 billion over the next ten years to equip ourselves with the capabilities needed to respond to growing cyber threats. The Strategy was informed by extensive stakeholder engagement and an expert Industry Advisory Panel.

Key initiatives include enhanced protections for critical infrastructure and systems of national significance, and greater support for businesses and individuals to develop their cyber security resilience. In addition, Australia's voluntary *Code of Practice: Securing the Internet of Things for Consumers* provides clear advice to businesses on the cyber security features we expect of Internet-connected devices available in Australia.

AUSTRALIAN CYBER SECURITY CENTRE GUIDANCE AND COVID-19

In response to an observed increase in COVID-19 themed malicious cyber activity, the Australian Cyber Security Centre (ACSC), part of the Australian Signals Directorate, issued a range of publicly available guidance and advice to help protect systems, data and personal information. These included advice to help critical infrastructure providers protect themselves from malicious cyber behaviour as key staff worked remotely, through to threat advice that Advanced Persistent Threat (APT) actors were actively targeting health sector organisations and medical research facilities. A joint statement by the ACSC and the Department of Foreign Affairs and Trade reaffirmed this in May 2020.

Cyber security engagement

Strengthening the region's cyber security strengthens our own. Enhancing the cyber security capability of Indo-Pacific partners is a focus of Australia's international cyber security engagement. We maintain a wide range of bilateral, multilateral and multi-stakeholder dialogues with regional and international stakeholders that enable us to meaningfully engage on cyber and technology-related issues of mutual interest, including cyber security.

Australia will continue to engage with regional partners to help mature cyber security and incident response capabilities and posture in the Indo-Pacific. This aligns with the *Boe Declaration on Regional Security* (agreed by Pacific Leaders in 2018), which confirmed cyber security as a key emerging security challenge for the region, and builds on the *ASEAN Leaders' Statement on Cybersecurity Cooperation* (agreed by ASEAN Leaders in 2018), and bilateral agreements with Singapore, Indonesia and Thailand. The ACSC leads operational and technical cyber security engagement, including with regional partners through the Pacific Cyber Security Operational Network (PaCSON) and the Asia Pacific Computer Emergency Response Team (APCERT).

Cooperative information sharing is fundamental to the ability of Australia and our international partners to effectively address the growing scale, sophistication and diversity of cyber threats. Australia is committed to fostering trusted cyber threat information sharing networks, such as PacSON and APCERT, which ensure all members are well placed to take informed cyber security actions in their respective countries. The ACSC will continue to produce public guidance and threat advice to assist Australia and our international partners to effectively address the most serious cyber security challenges.

Through our Cyber and Critical Technology Cooperation Program, Australia will support the delivery of tailored cyber security and incident response assistance to computer emergency response teams (CERTs) in Tonga, Vanuatu, Samoa, Fiji and the Security Operations Centre in Solomon Islands. This will boost our region's collective cyber security. These efforts will be complemented by the Pacific Fusion Centre, which provides cyber security media monitoring and strategic level analysis to empower Pacific decision makers to better identify and respond to regional cyber security threats.

Australia provides a voluntary contribution (in addition to our member-state contribution), to the International Telecommunication Union's (ITU) Development Sector each year to fund and implement activities such as cyber security training and capacity building in the Indo-Pacific region, with a particular focus on the Pacific. These activities are delivered in close collaboration with the ITU offices in Bangkok and Jakarta, and complemented by our support for the annual Policy and Regulatory Forum for the Pacific as a member of the Asia-Pacific Telecommunity. We also work with APEC members to advance the development of ICT infrastructure and services in the region and to promote a trusted and secure ICT environment through the APEC Telecommunications and Information Working Group (APECTEL).

THE PAPUA NEW GUINEA AUSTRALIA CYBER SECURITY COOPERATION MEMORANDUM OF UNDERSTANDING

The memorandum of understanding (MoU) demonstrates our commitment to ensuring cyber security underpins regional economic growth. Australia has committed $14 million (2018–19 to 2021–22) to protect critical Papua New Guinea networks. Our partnership also includes work to strengthen Papua New Guinea's cyber security governance arrangements, and build its cyber security community of practice by delivering ongoing accredited cyber security training for Papua New Guinea's government and industry staff. This work is enabling Papua New Guinea to better understand the cyber threat landscape and make informed decisions on its digital connectivity and telecommunications infrastructure needs.

CYBERCRIME

Australia will: strengthen cooperation for enhanced prevention, detection, investigation and prosecution of cybercrime

Australia will do this by:

Action 21. **Working** with international partners to strengthen our collective efforts to prevent, detect, investigate and prosecute cybercrime, with a focus on the Indo-Pacific

Action 22. **Supporting** the creation of a new model for international, cross-border lawful access to data

Action 23. **Promoting** the existing international legal framework on cybercrime and opposing efforts to weaken existing cybercrime law and norms, agreements and methods of collaboration

Cybercrime is a global threat, which undermines trust in cyberspace and causes significant economic and social costs. As connectivity increases dramatically, so too does Australia and the Indo-Pacific's collective exposure to cybercrime. Global cooperation is vital to respond to this challenge.

Australia, and our region, faces a worsening cybercrime landscape characterised by expanding threats, low barriers to entry, and increasingly resourceful actors, some of which are backed by states.

The modes and methods of cybercrime are relentlessly evolving. With access to increasingly sophisticated tools, like the dark web and anonymising technologies, cybercrime actors can adapt their techniques rapidly.

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 refers to crimes directed at computers, or crimes where computers facilitate an existing offence.

The range of COVID-19-themed scams, fraud attempts and deceptive email schemes observed by the Australian Cyber Security Centre (ACSC) in 2020 demonstrates that we remain an attractive target.

Australia remains committed to working with our international partners to prevent, detect, investigate and prosecute those partaking in criminal activity online, including on the dark web – wherever they may be located. Strengthening our capacity to combat cybercrime, both at home and overseas, enhances our region's collective security and resilience to cybercrime. Through the 2020 *Cyber Security Strategy*, and in line with the *National Strategy to Fight Transnational, Serious and Organised Crime*, Australia will prioritise support to victims of cybercrime, and work to ensure that our law enforcement agencies have the powers and technical capabilities to hold cyber criminals to account, and deter, disrupt and defeat the criminal exploitation of the dark web and anonymising technologies.

International operational cooperation

The Indo-Pacific remains particularly vulnerable to the threat posed by cybercriminals who look to exploit gaps in the region's legislative, policy, law enforcement and technical capacity. Australian law enforcement agencies engage international partners to support a regional response to cybercrime.

The Australian Federal Police's (AFP) partnerships with INTERPOL's Cyber Fusion Centre in Singapore and EUROPOL's European Cyber Crime Centre support the identification of new, imminent and evolving cybercrime threats.

Through the AFP, Australia will continue to build strong relationships with international partners to: improve cooperation on threat intelligence sharing assessment and analysis; trend monitoring; technical support for member countries; and, the identification of vulnerabilities, triage and disruption strategies.

State-sponsored cybercrime

State-sponsored cybercrime, where a state provides support or backing to individuals or groups undertaking criminal acts online, poses a serious risk to global security and financial systems. Profits from these criminal enterprises can be used to fund state activities including in contravention of international law and security frameworks (for example non-proliferation and financial sanctions).

The Indo-Pacific plays host to many of the world's most important crypto-currency exchanges, and will remain a lucrative target for resourceful state-sponsored cybercrime actors.

The Democratic People's Republic of Korea (North Korea) is responsible for increasingly sophisticated malicious cyber activities, including against financial institutions and crypto-currency exchanges in our region. In September 2019, the Panel of Experts assisting the UN Security Council North Korea Sanctions Committee noted that North Korea had raised as much as US$2 billion from such activities. Halting this flow of funds is vital to restricting North Korea's ability to fund illicit activities, including the development of nuclear and ballistic missile programs, and to counter sanctions evasion efforts by North Korea.

The investigative toolbox: data and encryption

Technology continues to expand the cybercrime threat landscape and, in turn, produce increasingly challenging circumstances in which to carry out criminal investigations.

The growth of global connectivity and increased reliance on cloud computing means that data once stored within Australia is now offshore. Lawful access to this data is vital for the effective investigation of cybercrime and other technology-enabled serious crimes. Traditionally, countries have relied on international crime cooperation mechanisms, such as mutual legal assistance, to lawfully obtain electronic data from overseas jurisdictions. However, the increased need for electronic evidence for all criminal offences is slowing these processes and affecting many countries' ability to investigate and prosecute crime.

Australia is committed to early adoption of new international cooperation mechanisms. We are negotiating a new agreement with the United States under the *United States Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), and are negotiating for a Second Additional Protocol to the *Council of Europe Convention on Cybercrime* (the Budapest Convention) for efficient cooperation on electronic evidence. New agreements with international partners for reciprocal access to electronic data would, when appropriate, bypass traditional mechanisms, while still ensuring appropriate protections and safeguards. This new model of modern, international crime cooperation would allow Australia to request data directly from foreign communications and technology companies in partner countries, rather than through governments.

Australia's commitment to an innovative cooperative framework for lawful access to data that also emphasises the importance of human rights, including freedom of expression, and the right to privacy, and the rule of law, models best practice for other countries in our region and internationally.

Australia also supports strong encryption as being fundamental to online security and trust. The technical challenge of achieving lawful access to encrypted or anonymised communications, and the legal challenge of obtaining the cooperation of the international communications industry, present new and increasingly difficult barriers to law enforcement and security agencies combating cybercrime. Australia's *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* sets out Australia's domestic legal approach to this challenge.

Australia will advocate regionally and internationally for policies and systems that enable access to encrypted or anonymised communications for law enforcement and national security purposes that:

- are transparent
- enable governments to work collaboratively with industry
- do not enable mass surveillance, the creation of decryption capabilities, or the implementation of so-called 'backdoors' that could undermine trust in digital communications
- are subject to legitimate independent oversight
- respect human rights and the rule of law.

AUSTRALIA'S *TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018*

The *Assistance and Access Act* introduced a modern, technologically neutral industry assistance framework. The framework establishes a structure for Australian agencies and industry to work together to address technological obstacles to investigations into serious crimes and national security threats. Agencies can request voluntary technical assistance or compel compulsory technical assistance from 'designated communications providers'. This includes information and communications technology companies that provide communications services or devices in Australia, irrespective of where they base their corporation, servers or manufacturing. There are many safeguards before technical assistance can be sought, including that it must be reasonable and proportionate, practicable and technically feasible, and not fundamentally weaken cybersecurity. To date, agencies have worked cooperatively with industry, with all requests managed on a voluntary basis.

International cybercrime frameworks

International cooperation is an essential part of Australia's efforts to combat cybercrime. No country can eliminate cybercrime alone – by its very nature, cybercrime is international, with victims, perpetrators, and evidence often located across many disparate jurisdictions. International cooperation, collaboration, information sharing, discussion and capacity building are vital to any meaningful response to the threat posed by cybercrime.

Australia has been a party to the Budapest Convention since 2013. The Budapest Convention is an established and proven mechanism that continues to bring considerable benefits to Australia and our region by harmonising and making interoperable the legal frameworks relating to: domestic cybercrime offences; electronic evidence collection by law enforcement; and, international cooperation and assistance.

BILATERAL ENGAGEMENT AND SUPPORT FOR THE BUDAPEST CONVENTION IN THE PACIFIC

Throughout the Pacific, the Australian Attorney-General's Department (AGD) has partnered with Pacific Island countries to strengthen domestic legislative frameworks to combat cybercrime in line with the Council of Europe Convention on Cybercrime (the Budapest Convention). Since 2014, AGD has partnered with Tonga, Fiji, Samoa, Vanuatu, Solomon Islands, Niue and Tuvalu to advance cybercrime law reform. AGD support has ranged from assistance in analysing compliance of existing laws with the Budapest Convention to assistance with drafting instructions for legislative reforms, the drafting of new domestic laws and reviewing draft legislation to ensure alignment with the Budapest Convention.

We continue to actively protect existing international law, frameworks and practices for cybercrime, uphold human rights, freedoms, and the rule of law, and oppose efforts to weaken them.

Through the United Nations (UN) Open-Ended Intergovernmental Experts Group to Conduct a Comprehensive Study of the Problem of Cybercrime, the Crime Congress, and the Commission on Crime Prevention and Criminal Justice, Australia will remain an active participant in broader international discussions to address and counter the full range of cybercrime. Australia will continue to support the UN criminal justice mandate based in Vienna and regional partners' attendance at these forums. We will also use these forums to continue to oppose online child sexual exploitation and abuse, building on the 2019 UN General Assembly Resolution *Countering child sexual exploitation and sexual abuse online*, led by Australia and adopted by consensus.[1]

Australia will continue to engage in multilateral discussions on cybercrime, consider appropriate proposals to address contemporary challenges, and support impartial, inclusive and expert-level dialogues aimed at combating cybercrime. We recognise the Budapest Convention as the most comprehensive and effective basis upon which to pursue a common international approach.

As the international community considers the elaboration of a UN convention of cybercrime (A/Res/74/247) Australia remains committed to advocating for a transparent, inclusive, and consensus-based process with multi-stakeholder participation. It will be important for any new instrument to build on existing and proven legal frameworks, such as the Budapest Convention, and ensure the protection of human rights, uphold the rule of law, and ensure an open, free and secure cyberspace.

1 UNGA Resolution A/RES/74/174, adopted 18 December 2019

Regional engagement and capacity building

Domestic capacity and capabilities, along with the ability to effectively cooperate internationally, are central to combating cybercrime. Australia, through our Cyber and Critical Technology Cooperation Program, will continue to support targeted and multifaceted capacity building in the policy, technical, operational and legal spheres, to support ASEAN countries and countries across the Pacific respond to the challenges posed by cybercrime.

Initiatives like the AFP-led Cyber Safety Pasifika and Cyber Safety Asia programs will assist regional law enforcement practitioners to develop further cybercrime-relevant skill sets, while providing broader community awareness and education regarding the risks of cybercrime.

These initiatives complement a range of initiatives led by the eSafety Commissioner and other Australian agencies aimed at mitigating a range of online harms (see Online Harms and Safety on page 59). Australia's broader law enforcement assistance programs, such as anti-money laundering assistance, will help build capacity to attack the profit that drives a large amount of cybercrime.

PACIFIC ISLANDS LAW OFFICERS' NETWORK (PILON) CYBERCRIME WORKING GROUP

Consistent with the Pacific Islands Forum's *Boe Declaration* priority focus on transnational crime and cybersecurity, the Australian Attorney-General's Department (AGD) has worked closely with the Council of Europe to support the Cybercrime Working Group of the Pacific Islands Law Officers' Network (PILON) to build awareness of the rising risks of cybercrime for Pacific communities. PILON is a network of senior legal and law enforcement officers from across the Pacific working together to contribute to a safe and secure Pacific by advancing key law and justice issues. Since 2017, PILON has facilitated annual workshops for over 80 Pacific policy makers, police and prosecutors, providing guidance on law reforms and building capacity to investigate and prosecute cybercrime. The Cybercrime Working Group has developed a mutual legal assistance handbook focusing on combating cybercrime and using electronic evidence. This handbook will provide criminal justice practitioners in the Pacific with practical information on the domestic and international mechanisms available to facilitate efficient and effective cooperation in criminal matters, and assistance accessing cross-border electronic evidence, a key component of Chapter III of the Budapest Convention.

ONLINE HARMS & SAFETY

Australia will: enable a safe and inclusive online environment

Australia will do this by:

Action 24. **Fostering** a safe and inclusive online environment and strengthening online safety through engagement with the global community

Action 25. **Countering** child sexual abuse and exploitation online through multilateral and multi-stakeholder cooperation

Action 26. **Preventing** terrorist and violent extremist exploitation of the Internet through multilateral and multi-stakeholder cooperation

Cyberspace and critical technologies provide significant opportunities to enhance social and cultural connections between communities in Australia, our region and the world. However, greater connectivity has also enabled extremist, harmful and unsafe online behaviour, conduct and content.

Cyberspace and critical technologies provide new opportunities to cause harm at an individual and societal level. Critical technologies have already been used maliciously to cause harm, such as through the generation of digitised impersonations or hyper-realistic digital falsifications of images, video and audio content ('deep fakes') to spread non-consensual pornography or image-based abuse. Terrorists and violent extremists from across the ideological spectrum also exploit the online environment to spread extreme and harmful propaganda, generate funding, radicalise individuals, and in severe cases, broadcast or incite physical acts of terror and hate.

Australia is committed to working with international partners including governments, industry, academia and civil society to tackle harmful and illegal online content and activity to foster a safe and inclusive online environment.

ONLINE HARMS

Online harms are activities that take place wholly or partially online that can damage an individual's social, emotional, psychological, financial or even physical safety. These harms can occur as a result of content, conduct, or contact (unwanted) and can include online activity or material that:

- involves the exploitation, grooming or abuse of children
- promotes, instructs, or incites terrorism, violent extremism or other criminal activity, or spreads or incites hate
- encourages or promotes violence or self-harm
- seeks to mislead, manipulate or defraud
- bullies, abuses, threatens, harasses, intimidates, humiliates, exploits, coerces or controls another person
- involves the non-consensual sharing of intimate images or videos
- is inappropriate for the age, maturity or background of children.

Engagement with the global community

Australia is an active contributor to international efforts to counter online harms. Through our bilateral and multilateral partnerships, we promote the rights, safety and dignity of individuals within the design, development and deployment of existing and emerging critical technologies. (See Human Rights on page 22; Ethics of Critical Technology on page 26). We develop and share world-leading online safety advice, advocate for a holistic approach to online safety, and support cooperative international efforts to improve outcomes for Australians and the international community.

To the extent possible, Australia seeks to ensure that our domestic legislation, regulatory frameworks and technological protections for the removal and prevention of harmful online content and conduct are consistent with international frameworks, and enable greater international interoperability and cooperation.

Recognising the potential of technology to improve online safety, Australia works with academia and industry across the world to promote innovative applications of critical technologies such as Artificial Intelligence and machine learning to counter harmful online material.

In addition, we recognise the importance of industry in cooperating with governments to develop and uphold codes of practice, industry standards and regulatory frameworks that support online safety and protect users from illegal and harmful uses of cyberspace and critical technology. Australia will strengthen engagement with the technology industry, and clearly articulate our expectations of them.

Australia's eSafety Commissioner

Establishing the eSafety Commissioner as the world's first national independent regulator for online safety reflects the Australian Government's significant commitment to protecting Australians online. The eSafety Commissioner has legislated powers to remove harmful and illegal online content including cyberbullying, image-based abuse, child sexual abuse material and notify service providers of abhorrent violent material present on their services.

Alongside its regulatory functions, eSafety provides citizen support services, research, early intervention and preventative education as part of a holistic approach to online safety. The eSafety Commissioner coordinates online safety efforts across Australia and plays an important international leadership role through targeted information sharing, coordination, collaboration and capacity building.

Safety by Design

eSafety promotes positive applications of current and emerging critical technologies, and proactively identifies and mitigates threats posed by its misuse through initiatives such as Safety by Design.

This online safety initiative seeks to influence the way that technology is designed, developed and used, shifting the responsibility for safety back onto technology platforms and providers. It provides realistic, actionable and achievable measures to better protect and safeguard users online, highlighting good practice and the tangible steps needed to make user safety considerations a routine element of product development cycles.

We recognise that this may impose additional costs to technology platforms and providers. It will be important that any additional cost is not unequally borne by consumers to ensure equitable access to technology that is safe and secure by design.

We are working with industry and global partners, collaboratively and constructively, to develop a suite of resources and guidance – including a Safety by Design assessment tool – to enable companies to understand potential harms, assess the risks to users on their platforms, and provide ideas and best practice innovation to build safety protection at the front end.

Preventing online child exploitation and abuse

Australia is committed to keeping children safe by preventing online child exploitation and abuse. Offenders are using advanced technologies and exploiting vulnerabilities on the Internet and dark web to harm children. Through multilateral and multi-stakeholder cooperation we work collaboratively to seek high-level commitment and operational engagement by governments, industry and civil society organisations to end online child sexual abuse and protect the rights of children. Australia works closely with international partners including INTERPOL and Europol, and uses global databases and platforms to access specialist expertise in our efforts to counter child abuse globally.

The Department of Home Affairs leads Australia's engagement on efforts to counter child sexual abuse in the Five Countries Partnership (Australia, Canada, New Zealand, the United Kingdom and the United States). In March 2020, the Five Country Ministers launched the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*, which were developed with six leading technology companies and in consultation with industry, civil society and academia. Australia has partnered with the WePROTECT Global Alliance, to drive collective industry action and promote implementation of the *Voluntary Principles*. Australia's partnership with WePROTECT is enhanced by the eSafety Commissioner's role as a board member.

WePROTECT GLOBAL ALLIANCE

An international not-for-profit organisation currently comprised of 97 governments, 25 technology companies and 30 civil society organisations.

Preventing terrorist and violent extremist exploitation of the internet

Terrorists and violent extremists from across the ideological spectrum exploit the online environment to spread extreme and harmful propaganda, generate funding, radicalise individuals, and in severe cases, broadcast or incite physical acts of terror and hate. Australia is committed to ensuring that opportunities for terrorist and violent extremist exploitation of the Internet are denied through concerted cooperation between foreign governments, the technology industry and other stakeholders.

Australia works closely with international partners to advocate for an increase in the ambition and pace of the technology industry's efforts to protect users from terrorist and violent extremist material online. These efforts should also ensure that the removal of this material does not frustrate law enforcement activity around the world.

Australia and partner governments seek comprehensive and sustained investment from the technology industry to: support research; improve transparency reporting; implement stricter live-streaming controls; reduce content take-down times; and achieve tangible improvements in the operation of the Global Internet Forum to Counter Terrorism.

AUSTRALIA, THE OSAKA G20 LEADERS' STATEMENT AND THE VOLUNTARY TRANSPARENCY REPORTING PROTOCOL

Australia led the Osaka G20 Leaders' Statement on *Preventing Exploitation of the Internet for Terrorism and Violent Extremism*, in support of New Zealand. It is a global call for online platforms and governments to work together to step up efforts to prevent, detect and remove terrorist and violent extremist content. G20 leaders called on online platforms to step up the ambition and pace of their efforts to prevent terrorist and violent extremist content from being streamed, uploaded, or re-uploaded and urged platforms to adhere to the core principle that the rule of law applies online as it does offline.

To implement the Osaka G20 Leaders' Statement, Australia partnered with the Organisation for Economic Cooperation and Development (OECD), co-financed by New Zealand and South Korea, to develop a Voluntary Transparency Reporting Protocol (VTRP). This project establishes a common protocol for online platforms to publicly report steps taken to prevent, detect and remove terrorist and violent extremist content.

The VTRP will deliver a benchmark of existing reporting practices by online platforms, establish metrics to measure progress and develop a common voluntary reporting protocol. This will deliver a Christchurch Call commitment to strengthen regular public reporting by online platforms on preventing terrorist and violent extremist content online, and support industry and governments to analyse, compare and react to emerging trends consistently across digital platforms.

PROSPERITY

AUSTRALIA'S GOAL:

Technology fosters sustainable economic growth and development

TO ACHIEVE THIS GOAL, AUSTRALIA WILL:

- Support a connected and prosperous Indo-Pacific comprised of independent sovereign states enabled by secure and economically viable critical technology
- Advocate for open, resilient, diverse and competitive international technology markets and supply chains
- Strengthen Australian research, industry and innovation through international cooperation
- Shape international critical technology standards that foster interoperability, innovation, transparency, diverse markets and security-by-design
- Promote the multi-stakeholder model of Internet governance
- Maximise economic growth by shaping an enabling environment for digital trade

Technological developments are now at the centre of economic change and growth. Advances in technology increase productivity and efficiency, create new economic activity and open access to new markets.

Australia's international engagement will seek to create the conditions in which we can maximise the opportunities of cyberspace and critical technology for our prosperity, and that of our region. We do this because Australia benefits from an Indo-Pacific region of stable, prosperous and sovereign states that cooperate on shared interests and are resilient to coercion.

We will support enhanced connectivity, particularly in the Indo-Pacific, and support the rules-based trading system to maximise our collective prosperity. Australia will oppose unnecessary bifurcation of global technology markets, taking into account Australia's national security and national interests.

We will advocate for open, resilient, diverse and competitive technology markets, and promote standards that foster safe, interoperable and secure technologies.

International engagement and cooperation multiplies our own scientific efforts and provides access to cutting-edge technology in a cost-effective way. Cyberspace and critical technologies have the potential to reshape our economy and sustain long-term economic prosperity for Australia and the Indo-Pacific.

REGIONAL CONNECTIVITY

Australia will: support a connected and prosperous Indo-Pacific comprised of independent sovereign states enabled by secure and economically viable critical technology

Australia will do this by:

Action 27. **Supporting** the development and deployment of secure, transparent and economically viable telecommunications infrastructure across the Indo-Pacific, and promoting policy and regulatory environments that enable partners to capitalise on this connectivity

Action 28. **Building** capacity across the Indo-Pacific to identify and address risks associated with the design, development and use of telecommunications infrastructure and critical technologies

Australia benefits from an Indo-Pacific region of stable, prosperous and sovereign states that cooperate on shared interests and are resilient to coercion. The development and deployment of current and next generation telecommunications infrastructure will provide significant economic and social dividends for our region. However, they also represent growing potential sources of influence, interference and coercion.

Powerful drivers of change are converging in the Indo-Pacific. Economic growth is shifting the distribution of power across the region, and cyberspace and critical technologies are increasingly central to geostrategic competition.

Some states may consider that they have to prioritise more immediate connectivity, over longer-term considerations of how this may impact their security and sovereignty. We will share Australia's expertise to enhance understanding of the risks associated with telecommunications infrastructure, and encourage partners to consider transparent, secure and sustainable solutions.

Pacific connectivity

While the Indo-Pacific has some of the world's most advanced digital economies, it is also home to countries whose digital development is still in its early stages. Connectivity remains a barrier to change with only 48.4 per cent of individuals in our region using the Internet.

We will support our neighbours through dialogue and investment in secure, safe and sustainable telecommunications infrastructure that advances their interests. We will position Australia as the partner of choice within our region on cyberspace and critical technology issues.

We have stepped up our connectivity efforts in the Pacific through the Coral Sea Cable System (CS2) and Solomon Islands Domestic Network (SIDN). The 4,700 kilometre fibre optic submarine cable system linking Sydney to Port Moresby and Honiara, and three regional sites in the Solomon Islands, is set to deliver high speed, low-latency communications infrastructure to Papua New Guinea and the Solomon Islands.

Alongside our investment, we will deliver capacity building that supports development of the policy and regulatory frameworks necessary to ensure our regional partners can harness connectivity in a safe, secure and sustainable manner. We will assist partners to: modernise their telecommunications markets to promote availability and affordability; reform regulatory environments to address issues such as competitiveness and privacy; promote accessible e-platforms for governance and education; and, enhance our partners' cyber security capacity (see Cyber Security on page 48).

AUSTRALIAN INFRASTRUCTURE FINANCING FACILITY FOR THE PACIFIC

On 1 July 2019, the Australian Government announced the new Australian Infrastructure Financing Facility for the Pacific (AIFFP). The $2 billion AIFFP significantly boosts Australia's support for infrastructure development in Pacific countries and Timor-Leste across a range of sectors including telecommunications. Through the AIFFP, Australia will fund high quality infrastructure that is responsive to the needs of partner governments, maximises local private sector participation, uses local labour, is climate and disaster resilient, promotes gender equality and social inclusion, and includes appropriate safeguards.

ASEAN connectivity

Australia supports a number of ASEAN connectivity initiatives, which are a priority for the ASEAN agenda. Australia has contributed significant funding to ASEAN connectivity including through the *Master Plan on ASEAN Connectivity 2025* (MPAC), a ten-year strategy adopted by ASEAN Leaders in 2016. MPAC was developed for ASEAN by Australian consultants and with Australian funding.

Australia also funded the development of ASEAN's Rolling Pipeline of Priority Infrastructure Projects, which includes green-fields ICT projects such as Thailand's 'ASEAN Digital Hub'. The hub aims to enhance bandwidth and create new cable routes throughout the region.

Australia will assist ASEAN develop a strategic plan to respond to the increasing centrality of critical technologies driven by enhanced connectivity. Innovations including cloud computing, the Internet of Things, open data and big data analytics, have already been widely adopted by ASEAN cities. Critical technologies have the potential to generate from $220 billion to $625 billion in annual economic impact in ASEAN by 2030. Australia supports ASEAN's connectivity agenda by working within ASEAN-centred architecture, including the East Asia Summit and ASEAN Regional Forum (ARF), to reinforce international law and norms in cyberspace. Australia will continue work with members of the Asia Pacific Telecommunity (APT) to deliver its mandate of promoting regional cooperation in radio communications, telecommunications and standards development, and reducing the digital divide within the Asia Pacific region.

COOPERATION WITH ASEAN

The *Plan of Action to Implement the ASEAN Australia Strategic Partnership 2020–2024* details our joint commitment to an open, secure, stable, accessible and peaceful ICT environment. Australia will continue to work closely with our ASEAN partners, including through biennial ASEAN–Australia Cyber Policy Dialogues.

SINGAPORE STATEMENT OF THE ASIA-PACIFIC MINISTERS ON CO-CREATING A CONNECTED DIGITAL FUTURE IN THE ASIA-PACIFIC

The June 2019 APT Asia-Pacific ICT Ministerial Meeting issued the Singapore Statement of the Asia-Pacific ICT Ministers on Co-creating a Connected Digital Future in the Asia-Pacific.

The statement covers five key focus areas which align closely with Australia's own priorities for the region:

1. Digital transformation, to promote economic growth through greater connectivity, digitalisation, transparency, market competition and consumer protection
2. Digital innovation and creativity, to help catalyse innovation and entrepreneurship in the development and utilisation of emerging ICTs
3. Digital community, to promote digital access in unserved and underserved regions, people in vulnerable groups and to embrace diversity through inclusive policies and reliable digital infrastructure
4. Digital trust, to encourage trusted and secure systems which promote the increased cybersecurity vigilance and foster a trusted and secure cyberspace
5. Digital capacity building and partnerships.

MARKETS & SUPPLY CHAINS

Australia will: advocate for open, resilient, diverse and competitive international technology markets and supply chains

Australia will do this by:

Action 29. **Working** with international and industry partners to encourage increased diversity in critical technology markets and supply chains

The next wave of critical technologies, including next generation telecommunications, novel applications of Artificial Intelligence (AI) and quantum computing, will be more complex, pervasive and interconnected than current technology. They will be integrated into every aspect of life, and have the potential to reshape our economies.

Technology is a key element of strategic competition. The increasing pace of change and centrality of technology, combined with complex and interdependent markets and supply chains, create growing challenges. Some countries are actively seeking dominance of critical technology markets and supply chains in pursuit of their geopolitical interests.

COVID-19 has demonstrated that diverse markets are essential. Australia, like many large economies, has significant innovation capabilities but remains a net technology importer.

Ensuring we have access to diverse, global technology markets for trade, and also to attract investment, is important to prompt the production of secure, cost-effective critical technologies, and fundamental to our national interests and our sovereignty. Nevertheless, the challenge of effecting this should not be understated at a time when the technology landscape is increasingly characterised by fewer and more dominant market players, which are centralised in a small number of countries.

Open, resilient, diverse and competitive markets

The ability of countries to protect their interests in national security and ultimately, their sovereignty may be significantly diminished where key markets are dominated by a small number of producers. The potential for monopolisation of critical technologies, or their components, may pose significant risks. The competition afforded by diverse markets prompts the creation and distribution of cost-effective technologies. Conversely, market monopolisation risks subjecting countries to varying degrees of economic coercion, and undermining their ability to participate meaningfully in global markets.

Transparency from suppliers regarding their practices, governance and supply chains, coupled with technological offerings that are secure by design, are central to the fundamental levels of trust required by Australia.

To ensure countries have access to diverse markets and can make informed choices about critical technologies, Australia will enhance our engagement with international and industry partners. While supporting diversified markets, we will advocate for the development of platforms and technologies that are interoperable, and will oppose unnecessary bifurcation or fragmentation of global markets. We will also build the capacity of our regional partners in the Indo-Pacific to navigate this increasingly complex environment.

TRUSTED MARKETS

Trust in suppliers within the market is critical to Australia's ability to maximise the benefits of critical technologies. We will promote policies that foster the creation of open, resilient, diverse and competitive markets, that deliver economic and security benefits.

Supply chains

Technology supply chains are increasingly global, interdependent and complex. This can promote greater responsiveness, lower costs, wider captive audiences and more diverse international participation. However, this complexity also means supply chain risks are increasingly difficult to identify and mitigate. COVID-19 further demonstrated that this increased level of interdependency can have a considerable impact on the safety, security and prosperity of all.

Transparency within supply chains is central to identifying and managing supply chain risks. This includes knowledge about ownership and manufacture. The need for transparency is now even greater as some states seek to leverage supply chain vulnerabilities for strategic advantage and as a possible vector for coercion.

We will also seek to promote cyber and critical technology capabilities that can strengthen supply chain resilience and sustainability. The Australian Signals Directorate provides guidance to cyber security practitioners, in government, critical infrastructure and large organisations about key cyber supply chain risks.

The value chains for the raw materials required to manufacture high-tech hardware are insecure due to market monopolies, trade restrictions and strategic competition. Australia has the capacity to add to market diversity by serving as an additional supplier of many critical minerals.

SUPPLY CHAIN PRINCIPLES

Australia will work with industry partners to produce voluntary principles for the security of critical technology supply chains. The principles will outline various factors that decision-makers across Government, States and Territories and industry are encouraged to consider when making investment decisions about the development, procurement or deployment of critical technologies. The principles will promote Australia's interests in security-by-design, transparency, autonomy and integrity, and will encourage adoption of secure critical technologies and broader diversity and competition in critical technology supply chains and markets. Australia will support governments and industry to adopt the principles.

RESEARCH, INDUSTRY & INNOVATION

Australia will: strengthen Australian research, industry and innovation through international cooperation

Australia will do this by:

Action 30. **Promoting** Australia's cyber security and critical technology industry and research

Action 31. **Attracting** investment and collaboration in Australian cyber security and critical technology industries and research

We are an innovative nation and a fast adopter of technology. International science and technology collaboration is a vital driver of Australian innovation. It enables our research community, including industry, academia and government, to be globally competitive and contribute to world-leading innovation.

International cooperation, especially in the early stages of research and development, allows for significant Australian input into market-shaping technological innovation. Australia's research community is world-leading in many critical technology sectors including advanced materials, the applied use of Artificial Intelligence (AI), autonomous navigation in GPS-denied areas, provable security and compliance, and quantum technologies.

Expanded efforts in science and technology diplomacy aim to promote Australia as a partner of choice for research collaboration, academic exchange programs and capacity building. We will strengthen our involvement in international research networks and promote Australian industry. International cooperation enhances our industry's global reputation and positions our research community to maintain foresight of emerging critical technologies. Australia is mindful of the need to ensure that international research collaboration addresses our strategic interests, and does not see Australian intellectual property diverted to support malign interests.

Overseas markets supply most of our technological requirements at a lower cost and more reliably than we could do alone. This is one of the reasons we remain open to trade and investment, and committed to competitive, open markets and collaborative research.

Taking Australia to the world

Science and technology lift the productivity and competitiveness of the economy. In the face of the most challenging economic circumstances in a century, capitalising on our relative strengths in science and technology innovation is critical for Australia's economic growth. Engaging with international research networks and promoting Australian innovation is key for growing Australia's future.

AUSTRALIA'S TARGETED TALENT EXCHANGE AND STUDENT PIPELINE

Australia recognises the benefit of targeted talent exchange and student pipelines with our international partners. CSIRO's Data61 has been actively developing such partnerships with countries like New Zealand, the United States, the United Kingdom, Germany, South Korea, Singapore and India to increase international cooperation on critical technology innovation, including cyber security, the Internet of Things, blockchain, AI and quantum computing.

The Government is committed to the commercialisation of Australian research and innovation. Global supply chains and export opportunities underpin Australia's cyber security and critical technology industry. They prompt Australian businesses to develop new capabilities and provide valuable avenues for commercialisation.

Close cooperation between Government, industry and business associations supports the identification of international market opportunities and the export of domestic innovation and capability. Initiatives such as the Landing Pads program, delivered by Austrade working in partnership with AustCyber, the Department of Defence and CSIRO, has supported cyber security and technology companies to access international opportunities.

To ensure Australian industry can continue to effectively capitalise on these opportunities, we will:

- promote Australian research internationally, including through Australian education exports, and support Australian involvement in international research networks where this is consistent with our national security interests
- support industry-led trade missions to increase the awareness and attractiveness of Australian companies to international customers and investors
- provide export support such as market intelligence and advice
- promote Australian companies as trusted partners within global supply chains
- monitor international technology markets and research networks to identify 'fast follower' opportunities.

Australia's interests in space technology

Space-based critical technologies are essential to our economy and security. We rely on space-based systems such as global navigation, communications and meteorological satellites to enable the full range of conveniences technology brings to daily life.

The Australian Space Agency (ASA) promotes Australian research, industry and innovation space-related critical technologies, and participates in international forums and agreements to strengthen Australia's space capability. ASA, in collaboration with CSIRO and the wider innovation ecosystem, will grow a globally significant Australian space industry that lifts the broader economy. This will be underpinned by strong international engagement, a central focus of the *Advancing Space: Australian Civil Space Strategy 2019–2028*.

THE AUSTRALIAN SPACE AGENCY

The Australian Space Agency's (ASA) Moon to Mars and International Space Investment (ISI) initiative form a core element of the *Advancing Space: Australian Civil Space Strategy 2019–2028*. This strategy sets the path to create up to 20,000 jobs and triple the size of the space sector in Australia to $12 billion by 2030.

The ISI provides $15 million over three years to strategic space projects that grow the Australian space industry. It will foster international collaboration with international space agencies and increase the capability and capacity of Australian industry and innovation in the space sector. Projects will target a minimum of 80 per cent of the investment being made in Australia.

In addition to the ISI, the Moon to Mars initiative provides $150 million over five years for Australian businesses and researchers to join NASA in returning to the Moon and then on to Mars. Demonstrator and pilot projects will showcase Australian innovation internationally, enabling new business ventures, revenue streams and markets.

Attracting international talent and investment

The Australian Government fosters Australian innovation in cyber and critical technology by:

- promoting Australia as a safe environment for foreign investment
- showcasing Australia as a location of choice for global cyber security and critical technology companies
- attracting international talent to Australia including through our world-class higher education institutions.

International participation in Australian research and innovation networks is fundamental to our ability to innovate and enhance our prosperity. It enables Australia to make cutting-edge research breakthroughs working in collaboration with others worldwide at the forefront of their field. Similarly, Foreign Direct Investment (FDI) drives economic growth, creates skilled jobs, improves access to overseas markets and enhances productivity.

Without foreign investment, production, employment and income would all be lower. Australian firms with foreign direct investment support one in 10 jobs in Australia. They also make a significant contribution to the one in five jobs that are trade-related. Nevertheless, we must be vigilant in ensuring partnerships and investments do not undermine Australia's national security.

Visa screening for critical technologies is one measure to prevent the unwanted transfer of knowledge which may jeopardise Australia's national security and international peace and stability. A screening process ensures that Australia remains a destination and partner of choice for legitimate international research and collaboration activities, while maintaining the integrity of our research, science, ideas, information and capabilities.

The design, development and use of critical technologies is a growing area of geostrategic competition. The Government works closely with Australian industry, universities and the research community to strengthen cyber security capabilities and build awareness of risks from foreign interference in Australian research. These efforts assist in safeguarding our research ecosystem from foreign interference and are targeted at Australian research networks to protect their integrity and the reliability of Australian companies as partners for international cooperation.

Foreign ownership of key assets, including businesses and entities involved in the development of critical technologies, requires careful consideration to balance our national security and economic needs. Australia will continue to adjust our FDI policies to ensure that they keep pace with emerging risks and global developments.

Changes to Australia's FDI regime will be communicated to provide certainty for investors. This will ensure that Australia continues to successfully attract levels of foreign investment that underpin our economic prosperity without compromising our national security. Proposed investments will be examined in accordance with Australia's open and transparent foreign investment framework.

AUSTRALIA'S FOREIGN INVESTMENT FRAMEWORK

On 5 June 2020, the Australian Government announced reforms to the *Foreign Acquisitions and Takeovers Act 1975*. The reforms preserve the principles of our system: that Australia welcomes foreign investment for the benefits it provides, but ensures that investments are not contrary to the national interest.

Australia's foreign investment framework will remain open, transparent and welcoming. Key elements of the reforms include:

- a new national security test for foreign investors who will be required to seek approval to start or acquire a direct interest in a 'national security business' – regardless of the value of the investment
- a time-bound 'call in' power enabling the Treasurer to review non-notifiable acquisitions that raise national security risks outside of proposed acquisitions relating to a 'national security business'
- a national security last resort power that provides the ability to impose or vary conditions and in extraordinary circumstances order disposal on national security grounds
- stronger enforcement options including the expansion of infringement notices and higher civil and criminal penalties
- measures to streamline approval for passive investors and investments into non-sensitive businesses.

CRITICAL TECHNOLOGY STANDARDS

Australia will: shape international critical technology standards that foster interoperability, innovation, transparency, diverse markets and security-by-design

Australia will do this by:

Action 32. **Increasing** efforts to shape global standards on the development, use and uptake of critical technology to promote interoperability, competition, innovation and diversity of suppliers

Action 33. **Engaging** with international partners and recognised standards development organisations to shape critical technology standards to promote security-by-design

The development of international standards on current and emerging critical technologies is increasingly important to economic competition and geopolitical security. This is due to their ability to shape technological trajectories, providing significant economic and strategic advantages to those who influence the development of technology standards.

Standards are the specifications, procedures and technical guidelines that ensure products, services and systems are safe, consistent, reliable, and interoperable. They ensure consistency for consumers, provide confidence in the safety and reliability of products, and when internationally harmonised, assist in reducing barriers to international trade.

Standard setting in emerging technologies has become increasingly strategic and important to the economic security of nations, and a crucial component of global technology competition. They can shape technological trajectories and advance the values and interests of those who set them. Despite the fact that many are developed and adopted voluntarily, standards can become mandatory through national legislation, associated regulations, and commercial contracts, enabling greater control over the intellectual property and value centres of global supply chains.

Why standards matter

The development and international harmonisation of critical technology standards play a vital role in Australia and the world's economic development. As the connective tissue between technology and the market, standards create trust and consistency, foster innovation and drive economic growth. Australia, along with many other countries, has maintained an industry-led, consensus-driven standards development process.

Some countries have notably increased the level of government involvement in support of standards development. National delegations to international standards bodies have grown in size and sophistication, and companies have, with the support of their governments, submitted an increasing number of domestic standards for consideration in international standards development organisations (SDOs) including the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO). This approach provides strategic and industrial advantages to states that drive the development of standards, particularly where companies are state-owned.

The increasing influence of critical technologies across society has also magnified the importance of the values underpinning their design, development and use. Through standards, values can be embedded to set a lasting trajectory for technological innovation and shape the way our society functions. Authoritarian regimes may seek to embed values in standards development that are contrary to Australia's liberal democratic values and national interests. Cognisant of this risk, we will work to shape the development and implementation of standards that promote technology consistent with human rights and our national interests.

STANDARDS AUSTRALIA

Standards Australia is Australia's National Standards Body and a member of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). It facilitates leadership and participation by Australian experts in ISO and IEC committees, with support and funding provided by the Australian Government for this purpose.

ASEAN-AUSTRALIA DIGITAL TRADE STANDARDS INITIATIVE

At the ASEAN-Australia Special Summit in Sydney in March 2018, the Prime Minister announced the ASEAN-Australia Digital Trade Standards Initiative to help ASEAN improve access to digital trade in the region. Following positive feedback from ASEAN, the Foreign Minister announced an extension to the project to 2022 to raise awareness about the role of international standards and address the key factors, which enable and inhibit digital trade across ASEAN and Australia.

Increasing Australia's international standards engagement

Australia will work with international partners to ensure the integrity of standards development systems and processes. We will seek to ensure that they remain open, commercially driven, and technology-neutral. Promoting security-by-design will be a key priority of this engagement.

Australia is committed to international standards development through existing multilateral and multi-stakeholder SDOs where appropriate. We will focus our engagement on strengthening international cooperation to ensure that SDOs are fit for purpose to address current challenges, accountable to member states, free from undue influence, and appropriately focused. Australia advocates for a transparent approach to rule setting in the development of standards, and stronger coordination between SDOs to reduce the duplication and overlap. These efforts assist in preventing divergent standards that splinter markets and reduce the benefits of harmonisation and innovation, or introduce vulnerabilities inimical to our national interests.

The Australian Government will continue to engage with the Australian standards community and business representatives to share information on the role of standards in critical technologies and developments impacting Australian business. Australia will also expand engagement with regional standards organisations across the Indo-Pacific.

Standards support diverse and competitive critical technology markets

Technical innovation is driven by trusted standards that encourage competition and diversity in critical technology markets. Australia will promote standards that are consistent with international trade and investment obligations, enable fair competition, encourage innovation and create economic opportunity.

Australia will work with our international partners to prevent standards that create barriers to trade and prevent interoperability of products and services globally. We will work to advance data standardisation and promote common frameworks for interoperability, privacy and security in critical technologies.

By embedding security-by-design as a core principle in critical technology standards, Australia will encourage greater competition based on security, incentivising suppliers to lift the overall security of critical technologies.

THE CODE OF PRACTICE – SECURING THE INTERNET OF THINGS FOR CONSUMERS

It is essential that internet-connected devices are secure-by-design and have sufficient security standards to defend against potential threats and malicious cyber activity. The *Code of Practice: Securing the Internet of Things for Consumers* represents a first step in the Australian Government's approach to improve the security of IoT devices in Australia.

As a key deliverable of *Australia's Cyber Security Strategy 2020*, the Code of Practice is a voluntary suite of measures the Government recommends industry adopt as the minimum standard for Internet of Things (IoT) devices. Comprised of 13 principles, the Code of Practice encourages security-by-design throughout the lifecycle of IoT devices.

The principles signal to domestic and international manufacturers the importance of protecting consumers and the security features expected of IoT devices available in Australia.

INTERNET GOVERNANCE

Australia will: promote the multi-stakeholder model of Internet governance

Australia will do this by:

Action 34. **Opposing** efforts to bring the technical management and governance of the Internet under government control

Action 35. **Supporting** and strengthening capacity for all stakeholders, including industry and civil society, to engage in multi-stakeholder Internet governance mechanisms

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.

Central to our interests in a peaceful and stable cyberspace is preserving the multi-stakeholder model of Internet governance. The multi-stakeholder system of Internet governance is a decentralised governance model. It places individuals, industry, non-commercial interests and governments on an equal level and allows for community-based policymaking.

The multi-stakeholder model recognises that all stakeholders have a valuable contribution to make to Internet governance discussions and decisions. It is a proven model for responding to complex policy and technical challenges associated with the development of the Internet. Current policy challenges include security, consumer protection, maintaining legitimate competition and managing cross-border data flows. This approach, by design, prevents any group (including states) from exerting undue influence over the Internet.

The multi-stakeholder model has guided the evolution of the Internet into a global network that has created significant economic opportunity and growth throughout the world. Changing this approach to allow any stakeholder to dominate the governance of the Internet puts at risk the connectivity and interoperability that is at the heart of the growth and utility of the Internet.

Continued evolution within a multi-stakeholder model

Like the Internet itself, the multi-stakeholder model must evolve to meet the challenges of administering this increasingly vital piece of global infrastructure. We will continue to work with all stakeholders to ensure that the multi-stakeholder model is sustained as the basis of global decision making for governance and technical policy issues related to the management of the Internet. While opposing government control of the Internet, we recognise that governments have expertise in public policy and are uniquely placed to bring a broad range of considerations to discussions about the future of the Internet.

Not all states support the multi-stakeholder model, and many would prefer to limit the ability of non-government stakeholders to influence decisions on the future of the Internet. This would enable the creation of an Internet that is more easily controlled by states, restricting Australia's ability to ensure cyberspace is safe and secure.

Australia opposes all attempts to bring governance and technical management of the Internet under the control of governments or into the multilateral system. Australia will support consensus-based forums such as the Internet Engineering Task Force, in promoting open, voluntary standards for the Internet.

Australia advocates for continuing, consensus-based improvement of existing mechanisms of multi-stakeholder Internet governance. We welcome increased discussion on how existing multi-stakeholder mechanisms can evolve, rather than advocating for the establishment of new mechanisms.

INTERNET GOVERNANCE

Australia is a strong supporter of an open, free, safe and secure Internet, and advocates for policy settings that support this position. 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).

Raising the capacity of stakeholders

To achieve these objectives, all stakeholders must have the capacity to meaningfully engage in multi-stakeholder Internet governance mechanisms. We will continue to raise awareness of Internet governance issues across the Indo-Pacific, and build the capacity of our regional partners to engage in multi-stakeholder mechanisms and forums. We will seek to raise awareness among international stakeholders about the unique Internet governance and cooperation challenges faced by Indo-Pacific countries.

Australia will also continue to strengthen and promote the capacity of civil society and industry to engage in Internet governance mechanisms. These groups play a fundamental role in the multi-stakeholder model of Internet governance, which is particularly important as this model continues to evolve. We will continue to engage with civil society and industry to ensure all stakeholders have the capacity to actively engage in these forums, and their voice is represented in international discussions on the future of the Internet.

THE MULTI-STAKEHOLDER MODEL

The multi-stakeholder model cannot be taken for granted. As the strategic importance of the Internet increases, so too does competition over how it is managed, and how it will evolve to meet the challenges of greater demand for safe and secure high-speed connectivity and new applications such as autonomous vehicles.

DIGITAL TRADE

Australia will: maximise economic growth by shaping an enabling environment for digital trade

Australia will do this by:

Action 36. **Pursuing** global trade rules that reduce barriers to digital trade and support the growth of an open and competitive economic environment

Action 37. **Securing** agreement to high-quality international trade rules and commitments that facilitate trade and protect consumers and their personal information

Digital trade is a fundamental driver of economic growth and presents significant opportunities as well as challenges for Australian businesses. Expenditure on digital goods and services, skills, equipment and the development and analysis of data are significant sources of economic activity. In turn, these activities are catalysts of the next wave of innovation and entrepreneurship in critical technologies.

Digital trade is not just about buying and selling goods and services online. It also encompasses the sale of products and services through digital technology; the import and export of digital hardware, software and services; and the flow of data across borders.

Australia relies on the use of digital technologies to facilitate trade and improve productivity. This includes through simplified digital customs procedures, e-signatures, e-payments and e-invoicing. Digital trade is an increasingly important way for Australia to trade with the rest of the world. Approximately half of Australian businesses are already engaged in the digital economy in some way, and this number is anticipated to grow.

Shaping an environment that enables digital trade

Australia seeks to shape an international environment that enables digital trade and reinforces the international rules-based trading system. Essential to this is the reduction of digital trade barriers, such as data localisation requirements and data flow restrictions. Australia pursues rules that facilitate trade by electronic means and build trust in the online environment through trade negotiations, including in the World Trade Organization (WTO), bilaterally and with regional groups. Australia advocates for such rules in a range of other international forums including the G20, the Asia-Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OECD).

Australia is committed to the development of multilateral rules on digital trade, the inclusion of digital trade rules within free trade agreements (FTAs), and is pioneering standalone digital trade agreements. We are chairing the WTO E-commerce Initiative to develop the first set of global digital trade rules, supported by Singapore and Japan as co-convenors. A majority of WTO members, representing well over 90 per cent of world trade, are now engaged in this process.

We advocate for the inclusion of e-commerce and digital trade rules within FTAs. Featuring in 14 of the 16 FTAs concluded by Australia, these rules facilitate trade by electronic means while preserving appropriate regulatory and policy space for Australia on important public policy issues. Subject to exceptions, including for national security, privacy protections, health, environment and prudential reasons, we advocate for rules that:

- support trade by prohibiting data localisation and allowing cross-border data flows
- promote secure and compatible electronic signature and authentication technology
- apply at least equivalent consumer protections online as offline, including in relation to personal information protection and discouraging spam
- create a safe online environment
- prohibit customs duties on electronic transmissions
- prohibit requirements to reveal source code.

Digital trade provisions will continue to be an important part of the FTAs that Australia negotiates. There remains enormous potential for further global digital trade growth. Australia will continue to pursue multilateral, regional and bilateral digital trade discussions.

ASEAN-AUSTRALIA DIGITAL TRADE STANDARDS INITIATIVE AND COVID-19

COVID-19 has reinforced the importance of ASEAN's digital agenda. In response, on 30 June 2020 at the Special ASEAN-Australia Foreign Ministers' Meeting on COVID-19, Foreign Minister Payne announced a $2 million extension to the ASEAN-Australia Digital Trade Standards Initiative. This initiative aims to build regional regulatory consistency in a context of rapid technological change. It provides a framework for Australia and ASEAN countries to cooperate in developing, adopting and using international standards that promotes digital trade and support inclusive economic growth in the region. The initiative will help ASEAN establish an open, vibrant and secure digital environment for e-commerce. Harmonised international standards across our region will help reduce the costs for Australian and ASEAN business' when exporting and importing products and services.

Data and governance

The data economy, which includes the collection, organisation and exchange of information, is an increasingly valuable area of global trade. Current and emerging critical technologies, such as the Internet of Things and machine learning are increasing the production and consumption of data, and rely on growing datasets to create value through applications such as targeted advertising. As such, data has become a commercial asset and a commodity for trade. This makes it more important than ever to balance the privacy, security and economic implications of the collection, use and transfer of data.

Australia advocates for the importance of data and personal information protection in cross-border data flows, especially where countries may take differing legal approaches to data protection. We will promote interoperability and compatibility between privacy regimes and endeavour to exchange information and best practice between jurisdictions, such as APEC's Cross-Border Privacy Rules system.

Australia recognises that government and industry have mutual responsibilities and interests in maximising the opportunities and mitigating the risks of cross-border data flows. We will continue to work with international partners to work towards compatible online data privacy laws, standards and governance mechanisms to protect data and personal information.

DIGITAL TECHNOLOGY TASKFORCE

The Digital Technology Taskforce within the Department of the Prime Minister and Cabinet works to ensure all Australians can benefit from digital technology. This includes considering how government can promote productivity gains through the take-up of digital technology across the Australian economy.

AUSTRALIA-SINGAPORE DIGITAL ECONOMY AGREEMENT

The Australia-Singapore Digital Economy Agreement (DEA) is Australia's first agreement of its kind. Signed on 6 August 2020, it sets new global benchmarks for trade rules to reduce barriers to digital trade and build an environment in which Australian businesses and consumers can benefit from digital trade and the digitalisation of the economy.

The DEA contains some of the most ambitious commitments on digital trade globally. Once ratified, the DEA will upgrade digital trade commitments under the Singapore-Australia Free Trade Agreement.

The DEA includes robust trade rules that, subject to relevant exceptions, establishes commitments on compatible e-invoicing and e-payment frameworks, and delivers benchmarks for improving safety and consumer experiences online.

The DEA also delivers a comprehensive framework for bilateral cooperation to help businesses and consumers capitalise on the digital economy. It includes cooperation commitments between Australia and Singapore on cyber security, artificial intelligence, international standards, Fintech and Regtech, data innovation, e-invoicing, e-certification for agricultural exports and imports, trade facilitation, personal information protection and digital identity.

ANNEXES

Annex A: Action Plan

CYBER & CRITICAL TECHNOLOGY DIPLOMACY

AUSTRALIA'S GOAL – Australia is a trusted and influential leader in cyber and critical technology diplomacy

	Australia will implement this Strategy by:	Lead Agency
CYBER & CRITICAL TECHNOLOGY DIPLOMACY	**1.** Prioritising and enhancing our cyber and critical technology diplomacy using a strategic and coordinated national approach	DFAT
	2. Shaping the design, development and use of cyberspace and critical technology in line with Australia's interests and values	DFAT
	3. Enhancing engagement with industry, civil society and the research community on cyberspace and critical technology	DFAT

VALUES

AUSTRALIA'S GOAL – Technology is used to uphold and protect liberal democratic values

	Australia will implement this Strategy by:	Lead Agency
DEMOCRATIC PRINCIPLES	**4.** Supporting applications of cyberspace and critical technologies that uphold and protect democratic principles and processes	DFAT
	5. Opposing the use of cyberspace and critical technologies to interfere, undermine or otherwise weaken democratic principles and processes	DFAT

	Australia will implement this Strategy by:		Lead Agency
HUMAN RIGHTS	**6.**	Promoting, protecting and upholding human rights online and in the design, development and use of critical technologies	AGD DFAT DITRDC eSafety
	7.	Opposing and condemning the use of cyberspace and critical technologies in a manner that violates human rights and freedoms	DFAT
	8.	Strengthening the capacity of states to meet their human rights obligations, and of other stakeholders to meet human rights responsibilities, online and in the design, development and use of critical technologies	DFAT
ETHICS OF CRITICAL TECHNOLOGY	**9.**	Engaging in multilateral forums and processes to shape global ethical principles and frameworks on critical technologies	DFAT DISER AGD
	10.	Sharing best practice approaches to the ethical design, development and use of critical technologies, consistent with international law including human rights	DFAT DISER AGD eSafety
	11.	Working with industry, civil society and the research community to develop non-binding ethical frameworks for critical technologies consistent with human rights	DFAT DISER AGD eSafety
DIVERSITY & GENDER EQUALITY	**12.**	Promoting greater diversity and inclusiveness in the design, development and use of cyberspace and critical technology	DFAT DITRDC eSafety
	13.	Advocating for gender equality and women's empowerment, and supporting greater awareness of the effect of cyberspace and critical technologies on gender equality	DFAT DITRDC eSafety
	14.	Embedding gender sensitivity and the meaningful inclusion and leadership by women and girls as key principles in Australia's cyber and critical technology capacity building	DFAT DITRDC eSafety

SECURITY

AUSTRALIA'S GOAL – SECURE, RESILIENT AND TRUSTED TECHNOLOGY			
	Australia will implement this Strategy by:		Lead Agency
INTERNATIONAL PEACE & STABILITY	**15.**	Setting clear expectations for responsible state behaviour	DFAT HA AGD
	16.	Deterring malicious activity enabled by critical technologies, including cyberspace, and responding when it is in our national interests	DFAT HA
	17.	Cooperating with other states to hold to account those that engage in unacceptable behaviour	DFAT HA ASD Defence
	18.	Implementing practical confidence building measures to promote international peace and stability and prevent conflict	DFAT HA ASD
DISINFORMATION & MISINFORMATION	**19.**	Building international partnerships with governments, industry and civil society to increase awareness of, and enhance resilience to, digital disinformation and misinformation	DFAT DITRDC HA
CYBER SECURITY	**20.**	Partnering in our region to strengthen collective cyber security and incident response capabilities	DFAT ASD/ACSC
CYBERCRIME	**21.**	Working with international partners to strengthen our collective efforts to prevent, detect, investigate and prosecute cybercrime with a focus on the Indo-Pacific	AGD AFP DFAT
	22.	Supporting the creation of a new model for international, cross-border lawful access to data	HA AFP AGD DFAT
	23.	Promoting the existing international legal framework on cybercrime and opposing efforts to weaken existing cybercrime law and norms, agreements and methods of collaboration	HA AGD DFAT

	Australia will implement this Strategy by:	Lead Agency
ONLINE HARMS & SAFETY	**24.** Fostering a safe and inclusive online environment and strengthening online safety through engagement with the global community	DITRDC eSafety
	25. Countering child sexual abuse and exploitation online through multilateral and multi-stakeholder cooperation	AFP HA DITRDC eSafety
	26. Preventing terrorist and violent extremist exploitation of the Internet through multilateral and multi-stakeholder cooperation	HA DFAT DITRDC eSafety

PROSPERITY

AUSTRALIA'S GOAL – Technology fosters sustainable economic growth and development

	Australia will implement this Strategy by:	Lead Agency
REGIONAL CONNECTIVITY	**27.** Supporting the development and deployment of secure, transparent and economically viable telecommunications infrastructure across the Indo-Pacific, and promoting policy and regulatory environments that enable partners to capitalise on this connectivity	DFAT HA DITRDC
	28. Building capacity across the Indo-Pacific to identify and address risks associated with the design, development and use of telecommunications infrastructure and critical technologies	DFAT DITRDC HA
MARKETS & SUPPLY CHAINS	**29.** Working with international and industry partners to encourage increased diversity in critical technology markets and supply chains	HA DFAT DISER

	Australia will implement this Strategy by:		Lead Agency
RESEARCH, INDUSTRY & INNOVATION	**30.**	Promoting Australia's cyber security and critical technology industry and research	DISER DFAT
	31.	Attracting investment and collaboration in Australian cyber security and critical technology industries and research	DISER AUSTRADE
CRITICAL TECHNOLOGY STANDARDS	**32.**	Increasing efforts to shape global standards on the development, use and uptake of critical technology to promote interoperability, competition, innovation and diversity of suppliers	DISER DITRDC HA DFAT
	33.	Engaging with international partners and recognised standards development organisations to shape critical technology standards to promote security-by-design	DISER DITRDC HA DFAT
INTERNET GOVERNANCE	**34.**	Opposing efforts to bring the technical management and governance of the Internet under government control	DITRDC DFAT
	35.	Supporting and strengthening capacity for all stakeholders, including industry and civil society, to engage in multi-stakeholder Internet governance mechanisms	DITRDC DFAT
DIGITAL TRADE	**36.**	Pursuing global trade rules that reduce barriers to digital trade and support the growth of an open and competitive economic environment	DFAT
	37.	Securing agreement to high quality international trade rules and commitments that facilitate trade and protect consumers and their personal information	DFAT

Annex B: Australia's position on how international law applies to State conduct in cyberspace

The international community recognises that existing international law – and in particular the UN Charter in its entirety – is applicable to State conduct in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. This includes, where applicable, the law regarding the use of force, international humanitarian law (IHL), international human rights law (IHRL), and the international law of State responsibility. The 2013 and 2015 reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), as adopted by the UN General Assembly, reflect this recognition.

Australia presented its position on the application of relevant international law to State conduct in cyberspace in its International Cyber Engagement Strategy (2017). This was further elaborated in 2019 through an 'International Law Supplement' to be read in conjunction with the 2017 Strategy. This Annex to the 2021 International Cyber and Critical Technology Engagement Strategy combines those positions and provides some updates.

In 2020, Australia also submitted a non-paper to the UN Open Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) containing a series of case studies on the application of international law in cyberspace.

The case studies seek to demonstrate that existing treaties and customary international law provide a comprehensive and robust framework to address the threats posed by state-generated or sponsored malicious cyber activity. In particular, international law provides victim States with a 'tool kit' to identify breaches of international legal obligations, attribute those acts to the responsible State, seek peaceful resolution of disputes and, where the victim State deems appropriate, take lawful measures in response. In this way, the application of existing international law to cyberspace can enhance international peace and security by increasing the predictability of State behaviour, reducing the possibility of conflict, minimising escalation and preventing misattribution. The case studies should be read in conjunction with this Annex.

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. To deepen understandings and set clear expectations, Australia encourages States to be transparent in how they interpret existing international law as it applies to State conduct in cyberspace. This Annex forms part of Australia's ongoing effort to make public its views on the application of international law.

1. The United Nations Charter, the law on the use of force (*jus ad bellum*) and the principle of non-intervention

The United Nations Charter (UN Charter) and associated rules of customary international law apply to activities conducted in cyberspace. Article 2(3) of the UN Charter requires States to seek the peaceful settlement of disputes and Article 2(4) prohibits the threat or use of force by a State against the territorial integrity or political independence of another State, or in any manner inconsistent with the purposes of the UN. These obligations – and the UN Charter in its entirety – apply in cyberspace as they do in the physical realm. They require States to resolve cyber incidents peacefully without escalation or resort to the threat or use of force.

The obligation to seek peaceful settlement of disputes does not impinge upon a State's inherent right to act in individual or collective self-defence in response to an armed attack. This right applies equally in the cyber domain as it does in the physical realm.

In determining whether a 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 activity, including for example whether the 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.

A use of force will be lawful when the territorial State consents, when it is authorised by the Security Council under Chapter VII of the UN Charter, or when it is taken pursuant to a State's inherent right of individual or collective self-defence in response to an armed attack, as recognised in Article 51 of the Charter.

Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber activities that constitute an armed attack and in respect of acts of self-defence that are carried out by cyber means. Thus, if a cyber activity – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged. Any use of force in self-defence must be necessary to repel the actual or imminent armed attack and be a proportionate response in scope, scale and duration. Any reliance on Article 51 must be reported directly to the UN Security Council.

The rapidity of cyber activities, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been noted by Australia in explaining its position on imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances. For example, in a speech to the University of Queensland in 2017, then Attorney-General, Senator the Hon. George Brandis QC, explained that:

> '[A] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts. This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy. Consider, for example, a threatened armed attack in the form of an offensive cyber operation, …which could cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second. Is it seriously to be suggested that a state has no right to take action before that split-second?'

Harmful conduct in cyberspace that does not constitute a use of force may still constitute a breach of the duty not to intervene in the internal or external affairs of another State. This obligation is encapsulated in Article 2(7) of the Charter and in customary international law.

A prohibited intervention is one that interferes by coercive means, either directly or indirectly, in matters that a State is permitted by the principle of State sovereignty to decide freely. Such matters include a State's economic, political, social systems and foreign policy. Coercive means are those that effectively deprive the State of the ability to control, decide upon or govern matters of an inherently sovereign nature. Accordingly, the use by a hostile State of cyber activities to manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of Parliament, or in the stability of States' financial systems would constitute a violation of the principle of non-intervention.

2. International humanitarian law (*jus in bello*) and international human rights law

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

Australia considers that, if a cyber activity rises to the same threshold as that of a kinetic 'attack' (or act of violence) under IHL, the rules governing such attacks during armed conflict will apply to those kinds of cyber activities. Applicable IHL rules will also apply to cyber activities in an armed conflict that do not constitute or rise to the level of an 'attack', including the principle of military necessity and the general protections afforded to the civilian population and individual civilians with respect to military operations.

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 activities 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.

International human rights law (IHRL) also applies to State conduct in cyberspace. Under IHRL, States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace. Subject to lawful derogations and limitations, States must ensure without distinction individuals' rights to privacy, freedom of expression and freedom of association online.

3. General principles of international law, including the law on State responsibility

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, applies to State behaviour in cyberspace. Under the law on State responsibility, there will be an internationally wrongful act of a State when its conduct in cyberspace – whether by act or omission – is attributable to it and constitutes a breach of one of its international obligations.

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.

Australia will, in its sole discretion, and based on its own judgement, attribute unlawful cyber activities to another State. In making such decisions, Australia relies on the assessments of its law enforcement and intelligence agencies, and consultations with its international partners. A cyber activity will be attributable to a State under international law where, for example, the activity was conducted by an organ of the State; by persons or entities exercising elements of governmental authority; or by non-State actors operating under the direction or control of the State.

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 (whether in cyberspace or through another means) under certain circumstances. Countermeasures are measures, which would otherwise be unlawful, taken to secure cessation of, or reparation for, the other State's unlawful conduct.

Countermeasures in cyberspace cannot amount to a use of force and must be proportionate. States are able to respond to other States' malicious activity with acts of retorsion, which are unfriendly acts that are not inconsistent with any of the State's international obligations.

If a State is the victim of harmful conduct in cyberspace, that State could be entitled to remedies in the form of restitution, compensation or satisfaction. In the cyber context, this may mean that the victim-State could, for example, seek replacement of damaged hardware or compensation for the foreseeable physical and financial losses resulting from the damage to servers, as well as assurances or guarantees of non-repetition.

Annex C: Norms for the responsible behaviour of States in cyberspace

From the report of the 2015 *UN Group of Governmental Experts on Developments 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.


Australian Government