ANNEX B

AUSTRALIAN IMPLEMENTATION OF NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

The international community – including the five permanent members of the United Nations (UN) Security Council (UNSC), and the UN General Assembly (UNGA) – have agreed a framework for responsible state behaviour in cyberspace (the Framework). The Framework affirms the application of existing international law to state conduct in cyberspace and articulates agreed norms of responsible state behaviour, while also recognising the need for confidence building measures, and coordinated capacity building.

The 2010, 2013 and 2015 reports of the United Nations Group of Governmental Experts (UNGGE) set out this framework (A/65/201; A/68/98; A/70/174). The UNGA subsequently considered – and endorsed, by consensus – the reports of the UNGGE (A/RES/65/41; A/RES/68/243; A/RES/70/237). Notably, in 2015, the UNGA called on all UN Members states '*To be guided in their use of information and communications technologies by the [UNGGE's] 2015 report*'. Many regional groups and leaders meetings have subsequently endorsed the UNGGE's reports (including, but not limited to: G20 2015, ASEAN Leaders' Statement 2018; ASEAN Communications Ministers 2018; EAS Leaders Statement 2018; CHOGM Declaration 2018).

Given this repeated high-level endorsement, it is clear that the international community expects countries to act consistently with the conclusions in the UNGGE reports. Australia reaffirms its commitment to act in accordance with the cumulative UNGGE reports from 2010, 2013 and 2015 (A/65/201; A/68/98; A/70/174).

With the intent of deepening common understandings and thereby increasing predictability and stability, this Fact Sheet contains a non-exhaustive list of the ways in which Australia observes the eleven norms in the 2015 UNGGE report. This Fact Sheet should be read in conjunction with the cumulative reports of the UNGGE. Other resources include the *International Security Chapter* of Australia's International Cyber Engagement Strategy, *Australia's position on how international law applies to state conduct in cyberspace* (2017) as supplemented by the *2019 International Law Supplement*, as well as information on Australia's $34 million *Cyber Cooperation Program*.

Norm	How Australia Observes the Norm
(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	Australia engages bilaterally, regionally and multilaterally to develop and apply measures to increase stability and security in the use of ICTs and to prevent ICT practices that are harmful or that may pose threats to international peace and security. A full overview of its activities can be found in the International Security Chapter of the 2019 Progress Report on implementation of *Australia's International Cyber Engagement Strategy*. Of particular note: at the UN, we are active participants of both the UN Group of Governmental Experts (UNGGE) and UN Open Ended Working

acknowledged to be harmful or that may pose threats to international peace and security	Group (OEWG). Regionally, we cooperate with Pacific Island and ASEAN neighbours, including through the ASEAN Regional Forum (ARF), Asia-Pacific Computer Emergency Response Team community (APCERT), as well as funding and participating in the Pacific Cyber Security Operational Network (PaCSCON). We have extensive bilateral cyber cooperation, including a number of established cyber policy dialogues. Australia's $34 million Cyber Cooperation Program has supported over 40 programs bilaterally and regionally to promote a peaceful and stable online environment and support regional partners to improve their cyber resilience. At the ARF, Australia and Malaysia led development of an ARF Cyber Points of Contact Directory. The Directory is a simple but practical confidence building measure that will consist of the relevant senior and working level contacts from participating ARF member countries. The Directory will facilitate direct, real time communication to prevent miscommunication, miscalculation and escalation in the event of cyber security incidents with the potential to impact regional security. Australia's International Cyber Engagement Strategy committed to diplomatic action to support an international cooperative architecture that promotes stability, and responds to unacceptable behaviour in cyberspace. In responding to malicious cyber activity, Australia will seek to engendered greater compliance with the rules and norms agreed at the UN. Any response will always be consistent with its obligations under domestic and international law, and designed to strengthen the rules-based international order. Our objective is to increase stability and security in the use of ICTs and to prevent ICT practices that are 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;	Australia has developed and published a Cyber Incident Management Arrangements (CIMA) for the Australian Governments (federal, state and territory). The CIMA outlines the inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for Australian Federal, State and Territory Governments' cooperation in response to national cyber incidents. It also defines a "National Cyber Incident". Australia maintains bilateral and multilateral relationships with CERT and cyber security counterparts globally to share information and cooperate during major cyber incidents. During a national cyber incident, the Australian Government's first priority is to mitigate the impact. Attribution of malicious activity is then necessary to enable a range of strategic response options. Depending on the seriousness and nature of an incident, Australia has the capability to attribute malicious

	cyber activity ranging from the broad category of adversary through to specific states and individuals. Australia has a well-developed process to guide and inform a decision by the Australian Government to make a public or private attribution disclosure. This process includes, but is not limited to, considering 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. The Australian Government has a comprehensive suite of strategic response options to deter and respond to unacceptable behaviour in cyberspace, encompassing diplomatic, economic, legal and law enforcement, defence-based, and private sector measures. To deepen common understandings, Australia has published information detailing how it considers cyber incidents and response options should be assessed under international law (see, e.g.: Australia's position on how international law applies to state conduct in cyberspace), including: • In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning. • When responding to a use of force, Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 of the UN Charter apply in respect of cyber operations that constitute an armed attack and in respect of acts of self-defence that are carried out by cyber means. Thus if a cyber operation – 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 (see, eg: 2019 International Law Supplement). Australia has also made public statements explaining its position on the concept of imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances.

	• If a state is a victim of unlawful 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) against the perpetrator state, 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. • Separate to countermeasures 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. Australia's transparency about the policies and procedures that inform its operational and strategic responses to cyber incidents are designed to promote common understandings, increase predictability, foster trust and reduces the risk of miscommunication during times of crisis.
(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs	This norm imposes a negative obligation. Australia does not knowingly allow its territory to be used for internationally wrongful acts using ICTs. Australia's commitment to act in accordance with this norm is demonstrated by: • A comprehensive set of offences to address cybercrime and the misuse of telecommunications (including those that either specifically target ICT systems, or the use of ICT systems to facilitate other traditional crime types such as fraud), which are consistent with the Council of Europe Convention on Cybercrime (the Budapest Convention), and are drafted in technology-neutral terms to accommodate advances in technology. • Public statements that Australia will act in accordance with the 2015 UNGGE norms and reports of the UNGGE (see: e.g.: Australia's International Cyber Engagement Strategy or Australia-China High Level Dialogue Joint Statement) • Publishing Australia's views on what constitutes an internationally wrongful act using ICTs, namely that - The 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 (see, e.g.: Australia's position on how international law applies to state conduct in cyberspace, 2019 International Law Supplement). Publishing Australia's views on what states should do if they are aware of an internationally wrongful act originating from or routed through its territory, namely that: • 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 see, e.g.: Australia's position on how international law applies to state conduct in cyberspace) By publishing these views, Australia seeks to promote common understandings, increase predictability, foster trust and reduces the risk of miscommunication during times of crisis.
(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;	**Cybercrime** Australia acceded to the Council of Europe Convention on Cybercrime (the Budapest Convention) in 2012. The Convention requires Parties to criminalise activity that undermines the confidentiality, integrity and availability of computer data and systems. It provides a basis for harmonised criminal offences, procedural and investigatory powers, and international cooperation to combat cybercrime. The Convention is deliberately technology-neutral, which allows it to evolve and maintain relevance as new technologies emerge. Accession to the Convention has assisted Australian law enforcement agencies to investigate, prosecute and disrupt cybercrime. The Convention is a valuable mechanism to strengthen international cooperation on

	cybercrime, particularly through its provisions on mutual legal assistance and establishing a 24/7 Network for Parties to assist investigations and secure electronic evidence efficiently. It works alongside and complements Australia's existing mechanisms for mutual legal assistance and law enforcement cooperation. Australia is actively engaged and at the forefront of efforts to combat cybercrime. For example, Australia participates in the development of a 2nd Additional Protocol to the Budapest Convention with the aim to supplement existing articles in the Budapest Convention itself and enhance international crime cooperation on cybercrime and electronic evidence gathering. Australia takes a constructive approach to UN work in Vienna to address cybercrime. In 2019 Australia and Mexico initiated and drove a resolution at the Commission on Crime Prevention and Criminal Justice (CCPCJ) on *Countering child sexual exploitation and sexual abuse online*. This resolution highlights the scale and changing nature of the threat posed by online child sexual exploitation and abuse. It calls for the criminalisation of child sexual exploitation and abuse online, and encourages improved cooperation between countries. The resolution acknowledges the importance of existing legal instruments, which require states to criminalise child sexual abuse and exploitation, and instruments which enable international cooperation to address these crimes. By doing so, the resolution acknowledges the importance of instruments like the Budapest Convention, which play this role. Australia also contributes to the UN Open-Ended Intergovernmental Expert Group on Cybercrime (IEG), formed under the CCPCJ in Vienna. The IEG is an expert-level group, with a mandate to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. The current work-plan of the IEG will cover discussions on legislation & frameworks for criminalisation, law enforcement & electronic evidence, international cooperation and prevention, with a stocktaking meeting in 2021 to discuss future work. The IEG and CCPCJ's useful work demonstrates the benefit of expert forums in Vienna. Australia cooperates closely with other countries in our region to strengthen capacity to address cybercrime. A key pillar of Australia's Cyber Cooperation Program is working with countries in the Indo-Pacific to improve cybercrime prevention, prosecution and international cooperation: specifically to strengthen legislative frameworks and institutional capacity to prevent, investigate and prosecute cybercrime. This includes (but is not limited to) projects partnering with Pacific Island Law Officer Network (PILON), the Australia Federal Police Cyber Safety Pasifika Program, the Jakarta Centre for

	Law Enforcement Cooperation (JCLEC), and the UN Office of Drugs and Crime (UNODC). **Terrorist use of ICTs** Australian works with the digital industry, regulatory agencies and international partners to identify, analyse, and disrupt violent extremist propaganda online. This includes increasing and optimising the channels for public reporting, including the Report Online Extremism tool and promoting existing channels on social media platforms; identifying content for referral to regulatory agencies or social media platforms; and working with partner countries to coordinate and maximise individual efforts. Australia also partners with a communications agency to undermine the appeal of violent extremist propaganda through the creation and curation of content that can discredit or trigger doubt in violent extremist messaging; promote positive messages that build trust with and within key Australian communities; and promote legal and constructive avenues for social justice. This includes fostering partnerships between influential individuals, groups and creative experts to design, produce and distribute content that challenges and promotes alternatives to violent extremism. Examples include activities and workshops designed to engage youth and give a greater number of people the skills to speak out against terrorist messaging at a local level, through the media and online to foster critical debate. Australia signed on to the Christchurch Call to Action, and following the Christchurch attacks, Prime Minister Morrison convened the Brisbane Summit to review priority domestic actions with industry, and as a result established a *Taskforce on Terrorist and Extreme Violent Material Online* comprising representatives from major online platforms, internet service providers and officials. Australia also led development and adoption of the G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT). This global commitment urged online platforms to meet citizens' expectations that they must not allow use of their platforms to facilitate terrorism and VECT. Building on this momentum, Australia is advocating across multiple fora to deepen international norms and develop common industry standards to prevent, detect, remove and deter terrorist and violent extremist content online. For example, it secured OECD member support to develop, in collaboration with industry and civil society, a voluntary transparency reporting protocol for online platforms to ensure a consistent and comparable approach to addressing terrorist and violent extremist content.

	This will help to measure progress and lay a pathway for strengthening international standards. As a consequence of this strong political consensus to call for collective action, and Australia's support for operationalising the Christchurch Call to Action, the Australian Government is working to progress action across multiple fora. This includes: advocating for a reformed Global Internet Forum on Counter-Terrorism (GIFCT) that is more independent, ambitious and transparent in its efforts to keep terrorist and VECT content off their platforms; supporting the Global Counter Terrorism Forum; and, collaborating with the Aqaba Process, the OECD and G7 members
(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;	Human rights apply online just as they do offline. Australia is a strong advocate of human rights online and a full overview of its activities can be found in the Human Rights Online Chapter of the 2019 Progress Report on implementation of *Australia's International Cyber Engagement Strategy*. Of particular note, at the 38th Session of the Human Rights Council (HRC38) in July 2018: Australia co-sponsored four resolutions promoting the protection of human rights online, including A/HRC/38/L.10/Rev.1 on the promotion, protection and enjoyment of human rights on the Internet. We also support and sponsor the work of Freedom Online Coalition and Digital Defenders. Australia joined the Freedom Online Coalition Joint Statement at HRC41 in June 2019 on free expression, peaceful assembly, and free association online. Australia has re-affirmed that international human rights law (IHRL) applies to the use of cyberspace. It has said that: • 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 (see 2019 International Law Supplement). Australia has strong national frameworks to ensure the promotion, protection and enjoyment of human rights online, including through the work of the Australian Information Commissioner, Human Rights Commissioner, and E-Safety Commissioner. The Australian Signals Directorate (ASD) is also subject to the Rules to Protect the Privacy of Australians made by the Minister for Defence
(f) A State should not conduct or knowingly support ICT activity contrary to its	This norm imposes a negative obligation.

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;	Australia does 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. Australia's commitment to act in accordance with this norm is demonstrated by: • Public statements that Australia will act in accordance with the 2015 UNGGE norms and reports of the UNGGE (see: e.g.: Australia's International Cyber Engagement Strategy or Australia-China High Level Dialogue Joint Statement) • Public statement about the conduct and authorisation of Australia's offensive cyber capabilities, which are always consistent with ASD's obligations at domestic and international law, and subject to a comprehensive review and oversight framework (see, eg: Mike Burgess, Director-General ASD, speech to the Lowy Institute, Offensive cyber and the people who do it; or Conduct and Authorisation of Offensive Cyber Capability in Support of Military Operations; or information published on the Accountability page on ASD's website). Australia's acknowledgment of these capabilities does not contradict its commitment to a peaceful and stable online environment. Instead, by being transparent about the legal frameworks that govern their use, we send an unambiguous message that states' activities in cyberspace have limitations and are subject to obligations, just as they are in the physical domain. Australia urges all countries likewise to be transparent and unequivocal in their commitment to develop and use ICTs in accordance with international law, as well as norms of responsible state behaviour agreed at the UN.
(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;	The Australian Government's Critical Infrastructure Centre brings together expertise and capability from across the Australian Government to manage the complex and evolving national security risks from foreign involvement in Australia's critical infrastructure. The Centre's initial focus is on assessing the risks of sabotage, espionage and coercion in the sectors of telecommunications, electricity, gas, water and ports. In 2018, the Australian Government passed the *Security of Critical Infrastructure Act 2018* (the Act) to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure. It contains a range of powers, functions and obligations that only apply in relation to specific critical infrastructure assets in the electricity, gas, water and ports sectors. The Act has three key elements: a register of critical infrastructure assets; an

	information gathering power; and, a Ministerial power to issue directions in cases where there are significant national security concerns that cannot be addressed through other means. The Act contains a number of safeguards and review mechanisms to ensure it is operating as intended. The Telecommunication and Other Legislation Act 2017, known as the Telecommunication Sector Security Reforms (TSSR), amends the *Telecommunications Act 1997* to establish a regulatory framework to better manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities. The TSSR reforms contain four key elements: a security obligation to protect networks and facilities from unauthorised access and interference; an obligation to notify the Government of changes to a network or facility, an information gathering power; and, a Ministerial directions power to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks. The Act contains a number of safeguards and review mechanisms to ensure it is operating as intended. The Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience was established by the Australian Government in 2003. It is Australia's primary national engagement mechanism for business-government information sharing and resilience building initiatives on critical infrastructure resilience. The TISN provides a secure environment for critical infrastructure owners and operators across eight sector groups to regularly share information and cooperate within and across sectors to address security and business continuity challenges. In July 2017, the Australian Government agreed with the recommendation of the 2017 Independent Intelligence Review that ASD become a statutory agency within the Defence portfolio. The review also recommended that ASD's legislative mandate be amended to explicitly recognise its national responsibilities for cyber security, including the provision of advice and assistance to businesses and the community and that it take formal responsibility for the ACSC. When the ACSC became part of ASD on 1 July 2018, it brought together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and support the economic, social and environmental prosperity of Australia in the digital age. ASD publishes cyber security advice for government, businesses and the community, including: • The Australia Government Information Security Manual, which outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.

	• Strategies to Mitigate Cyber Security Incidents, to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies are known as the Essential Eight, which provides organisations with a baseline to improve their cyber security resilience. • ASD's Stay Smart Online initiative provides advice to all Australians on how home internet users and small businesses can protect themselves from, and reduce the risk of, cyber security threats.
(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;	Upon receipt of an appropriate request for assistance, Australia will: • acknowledge receipt of the request; • determine, in a timely fashion, whether we have the capacity and resources to provide the assistance requested; • if we are able to assist, we will indicate the nature, scope and terms of the assistance that might be provided.
(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;	The ACSC has published Cyber Supply Chain Risk Management Guidance. The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the Act) introduced key reforms to enhance industry cooperation with law enforcement and security agencies and improve agencies' electronic surveillance powers. The measures enhance the existing ability of Australian agencies to undertake targeted, proportionate and independently oversighted surveillance activities. The Act expressly prohibits introduction of systemic weaknesses, or so-called 'backdoors'. Section 317B defines a systemic weakness/vulnerability as 'a weakness/vulnerability' that affects a whole class of technology…'. Further, Sections 317ZG and 317ZGA specify that providers cannot be required to build an interception, data retention or decryption capability (or build anything that removes a form of electronic protection, like encryption). Warrants are required to undertake surveillance or interception. The measures are subject to extensive oversight and independent review mechanisms. The Act equips agencies with the tools they need to effectively operate in the digital era and keep the Australian community safe - it is world leading in that it also contains extensive safeguards and protections that ensure the integrity of the supply chain so users can have confidence in ICT products. Any imposition of compulsory assistance obligations is subject to mandatory consultation with the affected communications provider.

	Australia is a member of the Wassenaar Arrangement, which promotes transparency, exchanges of views and information, and greater responsibility in transfers of conventional arms and dual-use goods and technologies with military applications. See also (j) below.
(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;	ASD has developed and implements a Responsible Release Principles for Cyber Security Vulnerabilities
(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.	This norm imposes a negative obligation. Australia does not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams (CERT) or cybersecurity incident response teams (CSIRT)) of another State. Australia does not use its national CERT to engage in malicious international activity. Australia's commitment to act in accordance with this norm is demonstrated by: • Public statements that Australia will act in accordance with the 2015 UNGGE norms and reports of the UNGGE (see: eg: Australia's International Cyber Engagement Strategy or Australia-China High Level Dialogue Joint Statement) • Public statement about the conduct and authorisation of Australia's offensive cyber capabilities, which are always consistent with ASD's obligations at domestic and international law, and subject to a comprehensive review and oversight framework (see, eg: Mike Burgess, Director-General ASD, speech to the Lowy Institute, Offensive cyber and the people who do it; or Conduct and Authorisation of Offensive Cyber Capability in Support of Military Operations; or information published on the Accountability page on ASD's website). • Its active participation in – and support for – regional and international CERT and incident response communities, including APCERT, PacSCON, the Forum of Incident Response Security Teams (FIRST), and others.