AUSTRALIA

AUSTRALIAN MISSION TO THE UNITED NATIONS E-mail australia@un.int

150 East 42nd Street, New York NY 10017-5612 Ph 212 - 351 6600 Fax 212 - 351 6610 www.AustraliaUN.org

AUSTRALIAN PAPER – OPEN ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, SEPTEMBER 2019

1. PURPOSE

1.1. This paper outlines the issues that Australia would like to see discussed at, and considered for inclusion in a subsequent report of, the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG).

2. BACKGROUND

2.1. In December 2018, the United National General Assembly (UNGA) established two processes to discuss responsible state behaviour in cyberspace: an inaugural OEWG (A/Res/73/27); and, a sixth Group of Governmental Experts (UNGGE) ((A/Res/73/266). The groups present an important opportunity to generate a meaningful impact on international peace and stability.

2.2. The UNGA resolution establishing the OEWG and the UNGA resolution establishing the UNGGE both welcomed the effective work of earlier UNGGEs and the 2010, 2013, 2015 UNGGE outcome reports (A/65/201; A/68/98; A/70/174). The UNGA had previously considered and endorsed, by consensus – the outcome reports of the UNGGE (A/RES/65/41; A/RES/68/243; A/RES/70/237) and, 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 welcomed the reports of the GGE (for example, but not limited to: G20 2015; CHOGM Declaration 2018; ASEAN Leaders' Statement 2018; ASEAN Communications Ministers 2018; and, EAS Leaders' Statement 2018).

2.3. Cumulatively the 2010, 2013 and 2015 UNGGE outcome reports affirm that existing international law – and in particular, the charter of the United Nations in its entirety – is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. The reports also articulate voluntary non-binding norms of responsible state behaviour, while recognising 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 a Framework for Responsible State Behaviour (the Framework).

3. AUSTRALIA IS GUIDED IN ITS USE OF ICTS BY THE UNGGE REPORTS

3.1. 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).

3.2. Recalling that 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*' (A/RES/70/237), annexed to this paper is an overview of how Australia observes and implements the four key pillars of the 2015 UNGGE Report.

a) **Annex A** - Australia's position on the application of **international law** to state conduct in cyberspace
b) **Annex B** – Overview of Australian implementation of **norms** of responsible state behaviour in cyberspace
c) **Annex C** – Examples of how Australia advances international cyber stability through **Confidence-Building Measures**
d) **Annex D** – **Capacity Building** and a summary of Australia's Cyber Cooperation Programme.

3.3. The 2015 UNGGE report articulated best practice activities, which many countries were/are already implementing. Australia encourages all countries to conduct a stocktake of ongoing activities that align with the 2015 UNGGE report, as well as to identify gaps and (if applicable) capacity required to fill those gaps. Such a stocktake, combined with a gap and capsitiy analysis, would usefully inform the work of the OEWG and UNGGE.

4. PROPOSED OEWG FOCUS (AND COMPLEMENTARITY WITH THE UNGGE)

4.1. The OEWG and UNGGE should build upon the effective work and consensus reports of prior UNGGEs (as welcomed by the OEWG's and UNGGE's respective establishing resolutions, the UNGA, regional fora and world leaders, para 2.2 refers).

4.2. The OEWG and UNGGE have separate mandates and should operate independently. However, noting the short timeframes allocated to the meetings of the two groups, and their shared objectives in advancing responsible states behaviour in cyberspace in the context of international security, Australia encourages good faith collaboration between the UNGGE and OEWG.

4.3. Australia has considered how best to harness the two groups' points of difference and composition most efficiently, while fostering independent but mutually re-enforcing and complementary outcomes that will have immediate real world impact. Our focus is facilitating practical action, not protracted negotiation.

4.4. Harnessing the OEWG's membership of all 193 UN Member States, the OEWG could:

a) seek views and perspectives on existing and potential threats in the sphere of information security and possible cooperative measures to address them (including application of international law, voluntary and non-binding norms of responsible state behaviour, confidence building measures (CBMs) and capacity building);
b) recalling that UNGA called on all states to be guided in their use of ICTs by the 2015 UNGGE report (A/RES/70/237; A/70/174), seek an update from the UN Member States on steps taken to implement the 2015 UNGGE report and any barriers to the same; and
c) taking into account the digital divide among the UN Member States, consider and make recommendations on how best to facilitate coordinated capacity building to implement the recommendations in the 2015 UNGE report.

4.5. Harnessing the expertise of the UNGGE experts, and recalling that UNGA has called on all states to be guided in their use of ICTs by the 2015 UNGGE report (A/RES/70/237; A/70/174), the UNGGE could:

a) develop practical guidance outlining steps states can take to implement the 11 norms of responsible state behaviour as articulated in the 2015 UNGGE report;
b) develop practical guidance outlining steps states can take to implement the CBMs as articulated in the 2015 UNGGE report; and
c) study further how international law applies to the use of ICT by States, with a view to including findings in the consensus report of the UNGGE, or in national annexes to the same (as provided for in the UNGGE's mandate; A/C.1/73/L.37).

4.6. Going forward, the practical guidance from the UNGGE report could be drawn upon by states seeking to address gaps in implementation identified in the OEWG process, utilising – as required – the capacity building mechanisms/recommendations identified in the OEWG report. This proposed approach respects the independent and separate mandates of the groups, while also encouraging complementary and mutually reinforcing outcomes.

4.7. Australia also encourages both groups to address gender issues, including the way in which women are differently and uniquely affected by conflict and threats to international peace and security, as well as the link between developments in the field of information and telecommunications in the context of international security and the Women, Peace and Security (WPS) agenda. In respect to the latter, Australia commends UNIDIR's recent report into gender balance in arms control, non-proliferation and disarmament diplomacy 'Still Behind the Curve', which notes that the UN First Committee has the lowest proportion of female diplomats of any of the UNGA's Main Committees. Australia will continue to take tangible steps to support the active and effective participation of women in multilateral discussions related to international security and disarmament.

5. NATIONAL EFFORTS TO PROMOTE A GLOBAL CULTURE OF CYBERSECURITY

5.1. Separate and in addition to the issues addressed in the OEWG and UNGGE mandates, Australia recognises the need for countries to take steps domestically to promote a global culture of cybersecurity. In this regard, we recall and commend the consensus resolutions listed below.

a) **A/RES/64/211** *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, which contains a voluntary self-assessment tool for national efforts to protect critical information infrastructures
b) ***A/RES/58/199*** *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* which contains a list of 11 elements for protecting critical information infrastructures
c) ***A/RES/57/239*** *Creation of a global culture of cybersecurity,* which contains a list of nine complementary elements to foster a global cultural of cybersecurity.

5.2. Australia is committed to promoting a global culture of cybersecurity pursuant to UNGA Resolutions A/RES/57/239, A/RES/58/199 and A/RES/64/211. Australia pursues a comprehensive and coordinated cyber agenda that draws on a wide range of multi-disciplinary expertise from across the Australian Government. **Annex E** provides a list and overview of key actors in the Australian cyber-ecosystem.

5.3. Australia considers that women's equal and active participation in the areas of science, technology, engineering and mathematics (STEM) is key to effectively promoting a global culture of cybersecurity. Likewise, Australia is committed to better addressing the gender digital divide and to equipping women to women manage technology risks and abuse. The documents listed below highlight key Australian efforts to address these issues. In sharing these documents we aim to foster mutual learning and best practice in this field.

a) The Australian Signals Directorate (ASD), the Australian Government's leading cyber security agency, has a wide range of initiatives that support gender equality within its workforce (see **Annex F** – Australian Signals Directorate - Women in Cyber)
b) The Australian Department of Industry, Science and Technology recently published a Strategy 'Advancing Women in STEM' (available at: www.industry.gov.au/womeninstem)
c) The Australian Academy of Science recently published a 'Women in STEM Decadal Plan' (available at: www.science.org.au/womeninstemplan)
d) The Australia Government funded OCED 'Bridging the Digital Gender Divide' report, which contains best practice recommendations for governments (available at: www.oecd.org/internet/bridging-the-digital-gender-divide.pdf)
e) Australia's Office of the eSafety Commissioner's eSafetyWomen initiative has a range of resources to help women manage technology risks and abuse (see **Annex G** – eSafetyWomen, or: www.esafety.gov.au/women)

ANNEX A

2017 - AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE

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

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

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

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

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

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

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

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

The IHL principle of proportionality prohibits the launching of an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

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

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

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

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

3. For cyber activities taking place outside of armed conflict, general principles of international law, including the law on state responsibility, apply.
It is a longstanding rule of international law that, if a state acts in violation of an international obligation, and that violation is attributable to the state, that state will be responsible for the violation.

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

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

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

2019 - SUPPLEMENT TO AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE

In the *International Cyber Engagement Strategy* (2017) (Strategy), Australia committed to periodically publish its position on the application of relevant international law to state conduct in cyberspace. The first such publication appeared in Annex A to the Strategy. This document is the second publication and is aimed at further elaborating Australia's position on applicable international law as expressed in the Strategy. As such, it should be read as a supplement to that document.

Application and development of international law

The Strategy recognised the well-established position that existing international law - including the UN Charter in its entirety - provides the framework for responsible state behaviour in cyberspace. The international community, including the permanent members of the United Nations (UN) Security Council recognised this in the 2013 and 2015 reports of the UN Group of Governmental Experts on the use of Information Communications Technologies in the Context of International Security (UNGGE), as adopted by the UN General Assembly. Australia also acknowledged that activities conducted in cyberspace raise new challenges for how international law applies. 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. The Strategy, and this supplement, form part of Australia's ongoing effort to make its views on the applicability of international law public.

The law on the use of force (jus ad bellum) and the principle of non-intervention

The United Nations Charter (Charter) and associated rules of customary international law apply to activities conducted in cyberspace. Article 2(3) of the 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. In the Strategy, Australia made clear that these obligations – and the UN Charter in its entirety, including those obligations, apply in cyberspace as they do in the physical realm.

A use of force will be lawful when the territorial state consents, 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 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. The rapidity of cyber attacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been raised by Australia in 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 (see Figure 1).

FIGURE 1 – IMMINENCE AND CYBER OPERATIONS

"[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 (and, of course, when I say 'armed attack', I mean that term in the strict sense of Article 51 of the Charter). The cyber operation 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?"

Attorney-General, Senator the Hon. George Brandis QC,
University of Queensland, 11 April 2017

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 (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), 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, and social systems, and foreign policy. Accordingly, as former UK Attorney-General Jeremy Wright outlined in 2018, the use by a hostile State of cyber operations 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.

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

The Strategy and the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), discussed the applicability of international humanitarian law (IHL) to cyber operations in armed conflict, including the principles of humanity, military necessity, proportionality and distinction. Australia considers that, if a cyber operation 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 operations. Applicable IHL rules will also apply to cyber operations 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.

International human rights law (IHRL) also applies to the use of cyberspace (see e.g. Figure 2). 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.

FIGURE 2 – COMMONWEALTH CYBER DECLARATION

"Recognising the potential for a free, open, inclusive and secure cyberspace to promote economic growth for all communities and to act as an enabler for realisation of the Sustainable Development Goals across the Commonwealth, we: ...

5. Affirm that the same rights that citizens have offline must also be protected online."

Commonwealth Heads of Government Declaration
20 April 2018

General principles of international law, including the law on state responsibility

In the Strategy, Australia recognised 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.

Australia will, in its sole discretion, and based on its own judgement, attribute unlawful cyber operations 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 (see e.g. Figure 3). A cyber operation will be attributable to a state under international law where, for example, the operation 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.

As outlined in the Strategy, 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) 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. 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 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.

ANNEX C

HOW AUSTRALIA ADVANCES INTERNATIONAL CYBER STABILITY THROUGH CONFIDENCE-BUILDING MEASURES

To enhance trust and cooperation and to reduce the risk of conflict, the 2013 and 2015 UNGGE Reports (A/68/98 and A/70/174 respectively) recommended states consider a number of Confidence Building Measures (CBMs) (extracted in table below). As recognised in the UNGGE reports, CBMs promote trust among states, helping to reduce the risk of conflict by increasing inter-state cooperation, and promoting transparency, predictability and stability.

CBMs comprise transparency measures, risk reduction measures and cooperative measures. They are one of the most important tools in states' diplomatic toolkits to strengthen international peace and security and maintain a peaceful and stable online environment. Australia is committed to partnering internationally to implement the CBMs recommended in the UNGGE Reports; below is a non-exhaustive list of Australia's efforts in this regard.

1. **Transparency Measures** provide insights into a country's activities.
    a. Australia's 2016 Cyber Security Strategy, 2016 Defence White Paper, 2017 Foreign Policy White Paper, and 2017 International Cyber Engagement Strategy together with its 2019 Progress Report are all examples of Australian transparency measures, as they clearly explain our goals, vision and planned actions.
    b. In its 2017 International Cyber Engagement Strategy (Strategy), Australia committed to periodically publish its position on the application of international law to state conduct in cyberspace. The first such publication appeared in Annex A to the Strategy, and was supplemented in 2019 by a second publication, which further elaborates Australia's position on applicable international law. By publishing these views, Australia seeks to promote common understanding, increase predictability, foster trust and reduces the risk of miscommunication during times of crisis.
    c. To foster trust, Australia has publicly outlined the legal framework and review mechanisms that apply to the conduct and authorisation of its offensive cyber capabilities in support of military operations (see: the Strategy, page 55). Australia's acknowledgment of its offensive cyber capabilities does not contradict its commitment to a peaceful and stable online environment. Rather, by being transparent about the legal frameworks and review mechanisms that govern their use, Australia sends 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 to be transparent and unequivocal in their commitment to develop and use ICTs in accordance with domestic and international law, as well as agreed norms of responsible state behaviour.

2. **Risk Reduction Measures** build confidence in countries' capacity to collaborate to respond to specific instances of malicious cyber activity without escalation to conflict.

    a. Australia is an active participant in ASEAN Regional Forum cyber risk reduction discussions including through the ARF Open Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies and the ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies.

    b. Together with Malaysia, Australia led efforts to develop an ARF Cyber Points of Contact Directory, which was agreed by Ministers at the 26th ARF on 2 August 2019 in Bangkok. The Directory will facilitate timely communication in the event of a serious cyber incident, thereby reducing the risk of miscommunication, miscalculation and the potential for conflict.

    c. Through its Cyber Cooperation Program, Australia supported the Asia Pacific Network Information Centre (APNIC) to mentor new and emerging CERTs in the Pacific in order to strengthen responses to specific instances of malicious cyber activity and enhance cyber security capacity. In 2018-2019, DFAT supported technical capability development of CERTs in Tonga and Vanuatu with direct support grants as part of the Cyber Cooperation Program, as well as funding the creation of the Security Operations Centre (SOC) in the Solomon Islands (see also 3(b)(i) below).

    d. In October 2018, ASD's ACSC was re-elected Chair of the APCERT Steering Committee. With fellow Steering Committee members (from China, India, Japan, Korea, Malaysia and Taiwan). APCERT is a key to building cyber security cooperation in the Asia Pacific region through information sharing and collaboration.

    e. Australia is an active participant of both the UN Group of Governmental Experts (UNGGE) and UN Open Ended Working Group (OEWG). In these fora, we will work to achieve complementary and meaningful outcomes that reduce the risk of conflict, strengthen international peace and security and maintain a peaceful and stable online environment.

3. **Cooperative Measures** promote collaboration between countries based on a mutual commitment to improve cyber resilience and reinforce a peaceful and stable online environment.

    a. Australia cooperates bilaterally with a wide range of states, including through a high tempo of regional and global bilateral visits and established cyber policy dialogues with ASEAN, China, India, Indonesia, Japan, and the Republic of Korea. We are also active participants in regional and multilateral cyber meetings. These visits, dialogues and meetings provide an opportunity to engage openly on national strategies and policies, best practices, decision-making processes, relevant national organisations and measures to improve international cooperation (policy, legislative, and operational).

    b. Through its Cyber Cooperation Program (Program), Australia works across the Indo-Pacific to improve cyber resilience and thereby promote international stability, while driving global economic growth and sustainable development. The Program supports Australia's commitment to deliver on the UN 2030 Agenda for Sustainable Development, which recognises the vital role of digital technologies to achieve a better and more sustainable future

for all. Australia has increased its investment through the Cyber Cooperation Program from $4 million in 2016 to $34 million out to 2023. Key initiatives delivered under the Program include:

i. Supporting establishment of the Pacific Cyber Security Operational Network (PaCSON) to share best practice across the Pacific on cyber incident response and build knowledge and awareness of cyber security threat information, tools, techniques and ideas (2017-2020);

ii. International cyber law courses for government legal advisers from ASEAN and the Pacific, jointly funded with Singapore and the Netherlands and delivered through Cyber Law International (2018-2020); and

iii. Tailored training across the ASEAN region to consider agreed norms of acceptable state behaviour in cyberspace as recommended by the 2013 and 2015 UNGGE reports, jointly funded with the UK and delivered through the Australian Strategic Policy Institute (2019-2020).

iv. DFAT's Cyber Bootcamp Project, which provides partners across the Indo-Pacific region with an opportunity to engage directly with policy and operational specialists from across Australia's public, private and academic sectors. Bootcamps aim to build confidence in countries' capacities to understand and engage with the full spectrum of cyber-related challenges, issues and opportunities within the region.

c. Under the Australia-Papua New Guinea (PNG) Cyber Security Memorandum of Understanding signed in 2018, Australia partnered with PNG to establish the PNG National Cyber Security Centre (NCSC). Australia will continue to collaborate with PNG to ensure the NCSC is a sustainable national capability, including through delivering training in cyber security governance, technical cyber security and incident response.

d. Together with Singapore, Australia led development of the 2018 EAS Leaders Statement on Deepening Cooperation in the Security of Information and Communications Technologies and of the Digital Economy, which affirmed EAS member states commitment to cooperate on a range of cyber and digital issues.

Australia will remain a vocal supporter of, and active player in, the development of CBMs at the bilateral, regional and international levels.

2013 GGE Report (A/68/98)	
OP 26 (a)	The exchange of views and information on a voluntary basis on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international cooperation. The extent of such information will be determined by the providing States. This information could be shared bilaterally, in regional groups or in other international forums;
OP 26 (b)	The creation of bilateral, regional and multilateral consultative frameworks for confidence-building, which could entail workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from State use of ICTs and how these incidents might develop and be managed;

OP 26 (c)	Enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms;
OP 26 (d)	Exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels;
OP 26 (e)	Increased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems. This could include guidelines and best practices among States against disruptions perpetrated by non-State actors;
OP 26 (f)	Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security.
2015 GGE Report (A/70/174)	
OP 16 (a)	The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;
OP 16 (b)	The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;
OP 16 (c)	Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;
OP 16 (d)	The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:
OP 16 (d)(i)	A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;

OP 16 (d)(ii)	The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;
OP 16 (d)(iii)	The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;
OP 16 (d)(iv)	The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.
OP 17 (a)	Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;
OP 17 (b)	Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;
OP 17 (c)	Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;
OP 17 (d)	Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;
OP 17 (e)	Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

ANNEX D

AUSTRALIA'S CYBER COOPERATION PROGRAMME

ABOUT THE PROGRAM

Australia's Cyber Cooperation Program works across the Indo-Pacific to promote a peaceful and stable online environment and improve cyber resilience. Established in 2016, the Program plays an important role in supporting Australia's international cyber engagement, which champions an open, free and secure cyberspace that protects national security and promotes international stability, while driving global economic growth and sustainable development.

The Program supports Australia's commitment to deliver on the United Nations 2030 Agenda for Sustainable Development, which recognises the vital role of digital technologies to achieve a better and more sustainable future for all.

Australia has increased its investment to the Cyber Cooperation Program from $4 million in 2016 to $34 million out to 2023. This increase in funding signals the importance Australia has placed on building cyber resilience across the Indo-Pacific region.

PROGRAM OUTCOMES

The Cyber Cooperation Program aims to equip countries in ASEAN and the Pacific with the capacity to respond to the challenges and opportunities that cyberspace presents. It has five areas of focus:

1. **International cyber stability framework**: promoting an understanding of how existing international law, norms and confidence building measures apply in cyberspace.
2. **Cybercrime prevention, prosecution and cooperation**: strengthening legislative frameworks and institutional capacity to prevent, investigate and prosecute cybercrime.
3. **Cyber incident response**: working with partners to establish and strengthen national and regional cyber incident response capability and coordinate and share cyber security threat information across the region.
4. **Best practice technology for development**: advocating for best practice use of technology for development by integrating cyber security by design and respect for human rights online.
5. **Human rights and democracy online**: advocating and protecting human rights and democracy online, including freedom of expression online.

PARTNERSHIPS

The success of the Cyber Cooperation Program is based on its strong partnerships model which sees Australia partner with industry, academia, civil society and like-minded donors to combine knowledge, expertise and resources to advance and protect our collective interests in cyberspace. To date, the Program has supported over 40 projects across ASEAN and the Pacific working with over 25 delivery partners.

ANNEX E

AUSTRALIAN CYBER GOVERNANCE

The below table outlines key Australian Government departments and agencies and bodies, organisations and independent statutory offices with cyber, digital and technology related responsibilities.

Government Department (A-Z) Statutory Body / Other	Responsible Minister & Head	Responsibilities	Key Resources/links
Attorney-General's Department	- The Hon Christian Porter MP, Attorney-General and Minister for Industrial Relations - Secretary, Mr Chris Moraitis	The Attorney-General's Department (AGD) supports the development of Australia's cyber security policies, including with respect to privacy, protective security, administration of criminal justice and oversight of intelligence, security and law enforcement agencies. AGD also provides advice to Government on the application of international law in cyberspace, assists Pacific Island countries to strengthen their cybercrime legislation and promotes accession to the Budapest Convention.	www.agd.gov.au
Australian Human Rights Commission	- Minister as above - Human Rights Commissioner, Mr Edward Santow	The Australian Human Rights Commission protects and promotes human rights in Australia and internationally. Human Rights apply online as they do offline.	www.humanrights.gov.au
Office of the Australian	- Minister as above - Australian Information Commissioner and	The Office of the Australian Information Commissioner (OAIC) is the independent national regulator for privacy and freedom of information.	Privacy Act 1998 Australian Privacy Principles

Information Commissioner	Privacy Commissioner, Ms Angelene Falk	OAIC administers the Australian Privacy Principles (or APPs) and the Notifiable Data Breaches scheme	Data Breach Notification Scheme
Office of the Inspector-General of Intelligence and Security	- Minister as above - Inspector-General of Intelligence and Security, the Hon Margaret Stone	The Inspector-General of Intelligence and Security is an independent statutory office holder who reviews the activities of Australia Intelligence Agencies, including the Australian Signals Directorate	www.igis.gov.au
Department of Communications and the Arts	- The Hon Paul Fletcher MP, Minister for Communications, Cyber Safety and the Arts - Secretary, Mr Mike Mrdak AO	The Department of Communications and the Arts (DoCA) provides strategic advice to Government on online safety policy and legislation. DoCA collaborates across government and industry to advocate for policy outcomes on national interest matters, including cyber security, that balance national security objectives with social and economic outcomes. DoCA also leads the Australian Government's engagement in international telecommunications and internet governance forums, including the International Telecommunication Union (ITU), Asia-Pacific Telecommunity (APT), Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), Internet Governance Forum (IGF), and Internet Corporation for Assigned Names and Numbers (ICANN).	Online Safety ➢ Online Content Scheme under Schedule 5 and 7 of the Broadcasting Services Act 1992 ➢ Enhancing Online Safety Act 2015 Information ➢ What we do: Internet Governance ➢ What we do: International Involvement
Australian Communications and Media Authority	- Minister as above - Ms Nerida O'Loughlin, Chair and Agency Head.	The Australian Communications and Media Authority (ACMA) is Australia's regulator for broadcasting, the internet, radiocommunications and telecommunications. The ACMA is committed to maximising the economic and social benefits of communications and media for Australia.	https://www.acma.gov.au/theACMA The Australian Communications and Media Authority Act 2005

			Broadcasting Services Act 1992 Radiocommunications Act 1992 The Telecommunications Act 1997 Interactive Gambling Act 2001
Office of the eSafety Commissioner	- Minister as above - eSafety Commissioner, Ms Julie Inman Grant	The eSafety Commissioner is committed to empowering all Australians to have safer, more positive experiences online. eSafety was established in 2015 with a mandate to coordinate and lead the online safety efforts across government, industry and the not-for profit community.	E-Safety Information Information for parents and families Information for women Information for older Australians Cyberbullying complaints Image based abuse complaints Offensive and illegal content complaints
Department of Defence	- Senator the Hon Linda Reynolds CSC, Minister for Defence	The Department of Defence's mission is to defend Australia and its national interests. Defence supports its networks through a modern, contemporary cybersecurity capability, contributes to Australia's whole-of-government cyber security efforts, and	2016 Defence White Paper

	- Secretary, Mr Greg Moriarty	undertakes cyber operations in support of approved military operations.	
Australian Signals Directorate	- Minister as above - Director-General ASD, Mr Mike Burgess	The Australian Signals Directorate (ASD) is the Government's lead operational cyber security agency. ASD seeks to make Australia the safest place to connect online by providing cyber security advice to the community, businesses and governments, and disrupting cybercriminals operating outside Australia. The Australian Cyber Security Centre (ACSC) is part of ASD. It possesses a comprehensive understanding of cyber threats, and provides advice and assistance to help Australians identify and manage cyber risk. When serious cyber incidents occur, ASD – through the ACSC – leads the Government response to help mitigate the threat and strengthen defences. Staff from Department of Home Affairs, AFP, ASIO, ACIC, ADF and the Defence Intelligence Organisation are co-located at ACSC.	www.cyber.gov.au www.asd.gov.au
Department of Foreign Affairs and Trade	- Senator the Hon Marise Payne, Minister for Foreign Affairs and Minister for Women - Secretary, Ms Frances Adamson	Through its 2017 International Cyber Engagement Strategy, DFAT (Ambassador for Cyber Affairs) is responsible for delivering Australia's comprehensive and coordinated international cyber affairs agenda, including through multilateral and bilateral advocacy. DFAT works closely with partners across the Australian Government to deliver a suite of initiatives under the Strategy's seven key themes: Digital Trade, Cyber Security, Cybercrime, International Security, Internet Governance & Cooperation, Human Rights & Democracy Online and Technology for Development.	Strategy/Policy ➢ Australia's International Cyber Engagement Strategy (2017) ➢ Progress Report (2019)

			International Law ➢ Australia's position on how international law applied to state conduct in cyberspace (2017) ➢ International Law Supplement (2019) Media ➢ Cyber Affairs ➢ Twitter – Australian Ambassador for Cyber Affairs
Austrade	- Senator the Hon Simon Birmingham, Minister for Trade, Tourism and Investment - CEO, Dr Stephanie Fahey	The Australian Trade and Investment Commission (Austrade) is the Australian Government's trade and investment promotion agency. Through its global network of over 80 offices in more than 40 overseas markets Austrade assists Australian technology companies to enter new markets, find new partners and customers and identify export opportunities. Austrade partners with industry and government stakeholders to promote Australian digital technology and cybersecurity capabilities globally. As well as providing export marketing services Austrade delivers the Australian Landing Pad Program in San Francisco, Shanghai, Tel Aviv, Berlin, and Singapore.	Trade: https://www.austrade.gov.au/Australian/export Investment: https://www.austrade.gov.au/International/invest Australian Landing Pads: https://www.austrade.gov.au/landingpads
Department of Home Affairs	- The Hon Peter Dutton MP, Minister for Home Affairs and	The Department of Home Affairs leads the development of national cyber security policy. Home Affairs also coordinates the implementation of Australia's 2016 Cyber Security Strategy and	https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security

	Minister for Immigration and Border Protection - Secretary, Mr Michael Pezzullo	Action Plan. This strategy sets out the Government's philosophy and program for meeting the dual challenges of the digital age – advancing and protecting Australia's interests online. The Department also has policy responsibility for cybercrime and online child sexual abuse offences under Part 10.6 and Part 10.7 of the Criminal Code. Home Affairs leads certain aspects of Australia's international advocacy to combat cybercrime, including representation for the Council of Europe Budapest Convention on Cybercrime and initiatives which relate to cross-border access to communications data . It also leads the development of policy on the cyber security of critical and emerging technologies, including leading the Government's efforts to lift the security in the Internet of Things. The Critical Infrastructure Centre (CIC) within the Department of Home Affairs addresses the national security risks from foreign involvement in Australia's critical infrastructure through direct ownership and third party contractual arrangements. The CIC coordinates expertise and capability from across the Australian Government to provide guidance to critical infrastructure owners and operators on mitigating these risks, including through the cyber vector, to Australia's critical infrastructure assets.	https://cicentre.gov.au/ https://www.tisn.gov.au/Pages/default.aspx
Australian Criminal Intelligence Commission	- Minister as above - CEO, Mr Michael Phelan APM	The Australian Criminal Intelligence Commission (ACIC) works within the Australian Cyber Security Centre to help build a stronger picture of the cybercrime landscape. The ACIC's role includes working with partners to assess and prioritise cybercrime threats impacting Australia.	https://www.acic.gov.au/about-crime/determinations#accordion-6
Australian Federal Police	- Minister as above	The Australian Federal Police (AFP) enforces Commonwealth criminal law and protects Commonwealth interests from criminal	

	- Commissioner Andrew Colvin	activity in Australia and overseas. AFP Cybercrime Operations coordinates and leads the investigation of serious and organised criminal cyber activity impacting Commonwealth Government departments, systems of national significance or the whole of the Australian economy.	
Department of Industry, Innovation and Science	- The Hon Karen Andrews MP, Minister for Industry, Science and Technology - Secretary, Dr Heather Smith PSM	The Department of Industry, Innovation and Science is responsible for cyber security industry development, cyber security research and development, and cyber security advice and protections for Australia's small to medium enterprises as part of business advice facilitation. DIIS is also responsible for digital economy and technology policy, with a specific focus on artificial intelligence. Noting many sector specific technology policy streams sit within other portfolios (e.g. medtech, agtech) and a range of specific technologies e.g. 5G, drones and Internet of Things also sit with other portfolios.	Australia's Tech Future
Commonwealth Scientific and Industrial Research Organisation	- Minister as above - Chief Executive CSIRO, Dr Larry Marshall	As Australia's national science research agency, the Commonwealth Scientific and Industrial Research Organisation (CSIRO) solves the greatest challenges using innovative science and technology. Within CSIRO, Data61 has established itself as a leading data science and engineering group, working with government and industry on digital and data driven opportunities including Internet of Things, artificial intelligence, machine learning, robotics, cyber security, confidential computing, big data and software and programming for the behavioural sciences	Data61
Department of the Prime Minister and Cabinet	- Prime Minister the Hon Scott Morrison MP	Prime Minister and Cabinet - Provide high quality policy advice and support to the Prime Minister, the Cabinet, Portfolio Ministers and	https://www.pmc.gov.au/cyber-security

	- Secretary, Philip Gaetjens	Assistant Ministers including through the coordination of government activities, policy development and program delivery.	
Department of the Treasury	- The Hon Josh Frydenberg MP, Treasurer - Secretary, Steven Kennedy	Treasury has policy responsibility for the Australian Government's business data requirements, including its registers.	
Australian Prudential Regulation Authority	- Minister as above - Chair, Mr Wayne Byres	The Australian Prudential Regulation Authority is an independent statutory authority that supervises institutions across banking, insurance and superannuation and promotes financial system stability in Australia. APRA belongs to the Council of Financial Regulators Cyber Security Working Group, chaired by the RBA.	www.apra.gov.au Information Security Requirements for all APRA-regulated entities
Australian Securities and Investments Commission	- Minister as above - Chair, Mr James Shipton	The Australian Securities and Investments Commission (ASIC) is Australia's integrated corporate, markets, financial services and consumer credit regulator. ASIC belongs to the Council of Financial Regulators Cyber Security Working Group, chaired by the RBA.	www.asic..gov.au Cyber Security and Directors Cyber Resilience Health Check Cyber resilience good practices
Australian Consumer and Competition Commission	- Minister, as above - Chair, Rod Sims	The Australian Competition and Consumer Commission (ACCC) is an independent Commonwealth statutory authority whose role is to enforce the *Competition and Consumer Act 2010* and a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians.	https://www.accc.gov.au/ ACCC Digital Platforms Inquiry Consumer data right legislation

			OECD Consumer policy: Internet of Things, Draft paper on enhancing the security of digital products, which will include a focus on product safety. ACCC compliance & enforcement policy & priorities

Australian Government
Australian Signals Directorate

ASD

ANNEX F

AUSTRALIAN SIGNALS DIRECTORATE – WOMEN IN CYBER

Women in Leadership

There is gender parity in ASD's Senior Executive Service, which was achieved in 2018, growing from an initial 30 percent within a year. In the ASD's Australian Cyber Security Centre, over fifty per cent of the Senior Executive Service are women. Additionally, there is strong representation of women in many of the core elements of ASD's cyber security mission, including:

- Cyber security operations and incident response
- Cyber security tradecraft analysis
- Media and communications
- Advice and assistance to government
- Emerging technologies, and
- International strategy and engagement.

Parenting Outreach

The ASD Parenting Outreach Program is run quarterly and provides an opportunity for parents in ASD to spend time with their work colleagues and our senior leadership team. All parents and their children are welcome.

The Parenting Outreach Program ensures that our parents, particularly those on parental leave, can engage with their teams, keep up to date on the latest workplace information relevant to their disciplines and be aware of current and future opportunities available to them.

Members of the Senior Executive Service host the Parenting Outreach sessions, and chat with the parents about their experiences of working and parenting. The structure of these events is flexible, and toys and games are provided for the children.

Women's Leadership Council

ASD's Women's Leadership Council aims to drive equal gender representation in ASD, ensuring we make best use of the talent pool available. Acknowledging that we are an organisation with a high number of technical roles, the Women's Leadership Council vision is to initiate and drive positive action around recruitment, recognition, retention and representation.

Girls Programming Network

ASD lead the Canberra chapter of the Girls Programming Network (GPN), which is a free quarterly coding workshop for up to 100 girls aged between 11 and 17. The GPN aims to inspire and support girls to consider careers in computing and technology. It is coordinated and run by female volunteers within ASD, other technical organisations and tertiary students. The workshops are suitable for all abilities and include coding training, mentoring and the opportunity to demonstrate new skills to parents and carers at the end of the day.

Curious Minds Program

ASD provides several mentors for the Curious Minds program, which encourages girls in year nine to year 11 to pursue careers in science, technology, engineering and maths (STEM) by matching them with female coaches who work in STEM fields.

In July 2019, ASD hosted a cyber/maths event for 63 girls in the Curious Minds program which included engaging workshops and problem solving challenges to inspire the girls to consider careers in STEM.

ASD Cyber EXP

ASD Cyber EXP is an interactive online program for high school and university students to gain experience points in a cyber-security incident response operation. The experience is based on real-life scenarios and provides a taste of what it is like on the front lines of cyber security within ASD.

All program content was designed to ensure gender balance so that students could see equal representation in technical and cyber roles.

Entry Level Programs offered by ASD

ASD offer a broad range of entry-level programs from work experience, apprenticeships, cadetships, undergraduate sponsorships and a graduate program. Some examples include:

- ASD sponsors civilian students studying a degree in Computing and Cyber Security at the University of New South Wales - Canberra Campus. The sponsorship provides full tuition fees and a bursary, along with paid work experience placements at ASD. Of the current program participants, 33 per cent are women, compared to the national average for ICT degrees of 20 per cent women.

- The ASD Graduate Program is a 12 month development program followed by an ongoing role in ASD on completion. Of our 2019 graduate cohort, 45 per cent are women.

ANNEX G

Safe access to technology is crucial for women so they can stay connected to family and friends, find information and access support.

eSafetyWomen helps women stay connected, safely.

All Australians deserve to be safe online. And yet 1 in 4 Australian women has experienced emotional abuse, and 1 in 6 Australian women has experienced physical violence from a current or former partner[1]. In the majority of cases this abuse and violence includes the use of technology to abuse, control and stalk[2].

eSafetyWomen is an initiative of the eSafety Commissioner, funded under the **Women's Safety Package to Stop the Violence**.

eSafetyWomen empowers Australian women to manage technology risks and abuse and take control of their online experiences through:

- The **eSafetyWomen website**—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.
- **eSafety face-to-face workshops**[3]—equipping frontline, specialist and support staff in the domestic violence sector, with the knowledge, skills and resources to better assist their clients protect themselves against online abuse.
- **eSafetyWomen—online training for frontline workers**—gives remote and time-poor workers access to in-depth training about technology- facilitated abuse, an extends the knowledge of workers who have completed face-to-face training.

[1] Australian Bureau of Statistics 2016, Personal Safety, cat. no. 4906.0.
[2] Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET (2015) ReCharge: women's technology safety, legal resources, research and training. National study findings 2015.
[3] In partnership with WESNET (and with support from the Department of Social Services).

6. Feedback from the frontline

"Very interesting, practical and relevant to our work."

"Fantastic training and great information, really easy to understand. Highlights how important it is for workers to be on top of technology and how to make women and children safe from people who misuse and abuse it."

Register for an eSafety workshop

Our free workshops are delivered Australia-wide. Visit our website to register your interest.

Visit esafety.gov.au/women

Twitter @eSafetyWomen

Access our online training, which can be undertaken in your own time at your own pace. Find out more at frontlineworkers.esafety.gov.au

How to reach us

General enquiries: enquiries@esafety.gov.au
Subscribe: esafety.gov.au/subscribe

Technology and online trends move at a rapid pace and it can be hard for busy parents to keep up. Our tips and advice on online safety for parents and carers are designed so they can learn about the digital environment and how to help their children navigate the online world confidently and safely.

Risks and concerns

Research tells us that a large number of parents (60%) are concerned that their child is being exposed to a range of risks by being online, such as accessing inappropriate content, contact with strangers and excessive screen time. Parents report they want more information on online safety, especially about how to help their child deal with negative online incidents.[1]

Advice for parents and carers

Our website is designed for parents and carers to learn about the benefits and risks of being online so they can help their children have safer online experiences.

We provide strategies for parents and carers to tackle the big issues, talk about tricky subjects and deal with issues as they come up. Our advice and tips are evidence-based and focus on current and emerging online safety issues, including:

- cyberbullying
- online pornography
- sending nudes and sexting
- time online
- gaming
- unwanted contact and grooming
- eSafety Guide to games, apps and social media.

The wesbite includes a range of resources:

- the Screen Smart Parent Tour — an interactive self-reflective tool for parents and carers with practical tips and advice
- information and tips from leading online safety experts
- latest research and facts about Australian children online
- a range of downloadable guides and tip sheets
- links to professional support and help for parents and their children.

esafety.gov.au/parents

[1] Survey commissioned by the eSafety Commissioner, June 2016, of 2,360 parents in Australia with children aged 8 to 17 years who access the internet.

Tips to help keep your child safe online

It is virtually impossible to stay on top of every new app and emerging issue, or to monitor your child 24/7. Safeguards like parental controls, filters and safe searches can help to screen content and set time limits.

However, the best way to positively influence your child's online wellbeing is by actively helping them to make sound decisions and manage online risks as they arise.

eSafety Parents encourages you to take proactive steps, such as to:

- Communicate openly — talk openly and regularly with your child about their online activities, how they connect with friends, who they talk with and the type of sites they visit.
- Get involved — explore and experience online content together. Research or set up your own social media accounts and apps to get a better feel for any online risks and age ratings. Play along in online gaming.
- Explore safety strategies together — get your child to actively think of ideas on how they can keep safe online and how to avoid content that could be harmful to them.
- Agree on ground rules in advance — set daily limits for screen time and device free rooms at home. Be clear about the types of sites or apps your child should not visit and personal information they should not share.
- Lead by example — reduce your own screen time and stick to the rules that apply to the family. Show that you care about your own personal information through privacy settings and the type of content you share.
- Encourage respectful behaviour — encourage your child to think carefully before they post, text or share and avoid posting things that may upset others. Remind them there is a real person at the other end.
- Develop a safety plan in case things go wrong — encourage your child to speak to you or another trusted adult if they encounter something online that makes them feel uncomfortable or distressed. Be aware of what you and your child can do in cases of cyberbullying through blocking and reporting. Parents can report serious cyberbullying to the eSafety Commissioner using our cyberbullying complaints form. esafety.gov.au/reportcyberbullying
- Get professional support — if your child is distressed and needs further help as a result of a negative online experience, seek professional help and support.

Where to go for help?

Kids Helpline

Provides free, 24/7 confidential online and phone counselling for children and young people aged 5 to 25 years. Phone 1800 55 1800 or visit Kidshelpline.com.au

eheadspace

Offers confidential, free and secure space where young people aged 12 to 25 or their family can chat, email or speak on the phone with a qualified youth mental health professional. Phone 1800 650 890 or visit eheadspace.org.au

Parentline

Each state or territory has a dedicated Parentline that offers counselling, information and a referral service. Opening hours vary by state.

Parentline (ACT) — 02 6287 3833
Parentline (NSW) — 1300 1300 52
Parentline (QLD and NT) — 1300 30 1300
Parent Helpline (SA) — 1300 364 100
Parent Line (TAS) — 1300 808 178
Parentline (VIC) — 13 22 89
Parenting WA Line (WA) — 1800 654 432

Women Influencing Tech Spaces (WITS) is an initiative of the eSafety Commissioner (eSafety) aimed at protecting and promoting women's voices online.

WITS wants to empower women with the psychological armour to counteract cyber abuse and interact online with impact, confidence and resilience.

About WITS

Every woman deserves to have a safe, positive and empowering experience online.

Every woman has the right to live without the fear, threat or experience of cyber abuse.

WITS uses the stories, skills and strategies of women to raise awareness of the insidious impacts of cyber abuse.

WITS shows that when women support each other, they can protect and promote their voices and together gain strength and solidarity.

7. Why women?

Social media can be a powerful tool to engage, connect, communicate, learn and grow.

Unfortunately, we know that women are more likely to be the targets of personal, sexual and gender- based cyber abuse than their male counterparts.

Cyber abuse is not a women's issue; it is a societal issue that disproportionately affects women.

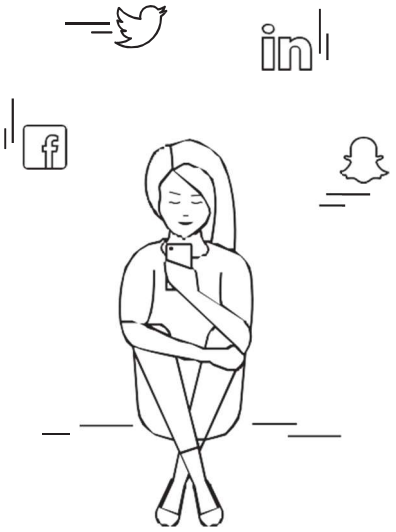
8. Buildingyourpsychologicalarmour

WITS helps women build their psychological armour by empowering them with resilience skills and strategies for coping with cyber abuse.

Finding help and support

Women who experience cyber abuse can access help and support in a number of ways:

- By reporting to a social media service's safety centre or eSafety. Depending on the platform, targets of abuse can generally also block, ignore or mute the abuse.
- By reviewing and updating social media privacy and security settings.
- By seeking help and support if in danger or experiencing distress.



WITS will contribute to creating a better online world for women.

Join and follow the WITS conversation #womenwithWITS esafety.gov.au/WITS

How to reach us

General enquiries: enquiries@esafety.gov.au
Subscribe: esafety.gov.au/subscribe

Social media: twitter.com/esafetyoffice
Media enquiries: media@esafety.gov.au