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.