16 April 2020

# Australia's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG)

*As requested by the Chair in his letter of 16 March 2020, this feedback is general in nature and does not purport to provide line-by-line commentary on the pre-draft. This feedback is not exhaustive and the right to provide further comment is reserved. As requested, feedback focuses on areas of potential agreement in the text, as well as providing suggestions to strengthen and streamline recommendations. Comments address each element of the Pre-draft and accompanying Non-paper, concluding with comments applicable to all.*

## A. Introduction

A1. Welcome the reflection in the Pre-draft that this OEWG builds on the foundation of the consensus reports and recommendations of the *Groups of Governmental Experts on the use of information communications technologies (ICTs) in the context of international security* (GGE) (paras. 5 and 6). Likewise, welcome the explanation of the complementary and interdependent nature of each of the subsequent sections (para. 12).

A2. Strongly support the recognition in the Pre-draft that development and use of ICTs have implications for all three pillars of the United Nations' work (para. 10), while simultaneously limiting the focus of the OEWG Report (the Report) to only those issues within the OEWG's mandate (para. 10). Caution against references to the "unique" nature of the OEWG (para. 6 et al), given ongoing discussions in other forums (see, e.g.: *UNODA Background Paper on existing UN bodies and processes related to the mandate*, available on the OEWG's website).

A3. Welcome the recognition in the Pre-draft that the OEWG benefited from multi-stakeholder exchanges (para. 7). Likewise welcome references to gender, including the need to encourage meaningful participation of women in discussions such as the OEWG (para. 9).

A4. Recalling interventions by several delegations (including Australia) that ICTs have had, and continue to have, a positive transformative impact in both the military and civilian contexts (para. 3). The OEWG Report should reflect that it is not the development or use of ICTs by militaries that is of concern. Rather, of concern is the use of ICTs in a manner inconsistent with the maintenance of international peace and security; A/RES/70/237 provides consensus language to this effect.

**B. Existing and Potential Threats**

B1. Paragraph 15 (and paragraph 3, discussed above) of the Pre-draft should be revised taking into account comment A4 above. The Report should build upon paragraph 4 of the 2015 GGE Report (A/70/174) with the following amendments: *"[A] growing number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts is ~~becoming more~~ likely."*

B2. We recall that GGE reports refrained from listing specific types of critical infrastructure. The Pre-draft notes complications arising from different national priorities and methods of categorisation (para. 19). In addition to sharing this concern, we are reticent to emphasise the severity of threats to particular categories of critical infrastructure, lest it be seen to implicitly condone malicious activity against a category not specified. That said, we see value in the Report drawing attention to the increased threat that cyberspace will be exploited by malicious actors for purposes inconsistent with international peace and security during times of global crisis. For example, paragraph 19 of the Pre-draft could express concern about the potential for increased exploitative state-sponsored malicious cyber activity that is inconsistent with international peace and security during global crises, including vis-à-vis critical infrastructure. Noting, with concern, open source reports of disruption by cyber means of critical infrastructure (including healthcare/medical services, facilities and systems, and crisis response organisations) during the COVID-19 global pandemic.

B3. Strongly support the acknowledgment in the Pre-draft that measures to promote responsible state behaviour in cyberspace should remain technology neutral (para. 18). Likewise welcome the clarity in the Pre-draft that the subsequent sections of the Report provide recommendations to address the threats so discussed (para. 21).

**C. International Law**

C1 Strongly support the reaffirmation in the Pre-draft that international law, including the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.

C2 Recalling the consensus among OEWG delegations that the question '*if* international law applies to state conduct in cyberspace' has been resolved in the affirmative and that the focus is now on *how* it applies. delegations discussed two paths to resolve this question. The *first* path (of which Australia is a proponent) is premised on the basis that – if adhered to – existing international law (complemented by voluntary norms of responsible state behaviour, confidence building measures and capacity building) provides a robust framework to address the threats posed by state-generated or state-sponsored malicious

cyber activity. The way forward is for States to publicly articulate views on international law's application and act consistently with those positions (in both responsible use of ICTs and responses to irresponsible uses of ICTs). If States are committed, this process could quickly deliver clarity and deepen common understandings on key questions of how international law applies to state conduct in cyberspace as well as contributing to the development of applicable customary international law. This path aims to avoid the protracted negotiations necessitated by the second path and the risk of erosion of the full suite of rights, obligations and protections afforded by existing international law. The *second* path to resolving the question of 'how' international law applies is premised on the basis that new international laws are required. In any event, many delegations supporting the second path acknowledged that articulating views on international law's application (i.e. the first path) would provide the foundations for – and therefore necessarily precede – the second path.

C3. As discussed in paragraph Y1, while preferable for the Report to reflect only consensus reached during discussions, should there be support for the Report to also serve as a record of discussions, it should more clearly articulate both paths (para. 26 cf: paras. 27-29), and note that contested issues (see, eg: para. 27) could be resolved under either path. In that instance, the Report should also reflect that, regardless of the path taken, the first step towards both paths is for States to develop and share national views on how existing international law applies (para. 30).

C4. In the context of state responsibility (para. 24), the Report should make clear that the customary international law on state responsibility provides that a State will be responsible for an internationally wrongful act where there is conduct that is attributable to it and that conduct constitutes a breach of its international obligations. The Report should make the distinction between different attribution assessments, including factual attribution assessments (which includes an assessment of technical and other contextual information) and legal attribution assessments (where there has been a breach of international law and/or domestic law), as well as the political decision to act – publicly or privately – on those attribution assessments. It may be more appropriate for this observation to be included in the section on Rules, Norms and Principles of Responsible State Behaviour (referencing norm 13(b) from the 2015 GGE report).

C5. Strongly support the text in the Pre-draft on international humanitarian law (IHL) (para. 25). To further emphasise that international law ensures predictability and stability, and that IHL does not encourage militarisation of cyberspace or legitimise conflict, the text emphasising UN Charter obligations (such as settlement of disputes by peaceful means and refraining from the use of force (currently para. 32)) should immediately precede the text on IHL (currently para. 25).

C6. The Report should elaborate more on mechanisms provided under the UN Charter to resolve disputes peacefully and address threats to international peace and security (including referring to Chapters VI, VII and XIV of the UN Charter) and make clear that these mechanisms are available with respect to disputes arising from state activities in cyberspace (para. 32).

**D. Rules, Norms and Principles for responsible state behaviour**

D1. Welcome acknowledgement in the Pre-draft that voluntary norms do not replace States' obligations under international law (chapeau). To emphasise this point, the Report should add "(which is binding)" after the references to "international law" in the second paragraph of the chapeau to this section and in paragraph 34. The Report should further emphasise that, when considering the application of the voluntary non-binding norms, States must simultaneously consider and respect their obligations under existing international law, which are binding.

D2. The Report also affords an opportunity to resolve a common mischaracterisation between the so called 'normative framework for responsible state behaviour in cyberspace' (the Framework) and 'voluntary non-binding norms' (norms); the norms being just one element of the Framework. A chapeau to the operative section of the Report should clarify that the normative framework of responsible state behaviour in cyberspace comprises: international law, which is binding; voluntary non-binding norms; confidence building measures; and, capacity building. The Report should then underline that each element of the Framework is mutually reinforcing and that no one element of the Framework – nor the sections of the Report that follow – should be considered in isolation (para. 12).

D3. Welcome reaffirmation in the Pre-draft of consensus support for the 11 norms of responsible state behaviour from the 2015 GGE report (para. 35), as well as consensus support among delegations of the need to promote awareness and support implementation of these existing norms (para. 37). The norms in the 2015 GGE report, remain the only norms endorsed by consensus by all UN Member States (A/Res/70/237) and therefore provide the natural starting point for a consensus based Report. Development of roadmaps and/or guidance to assist in norm implementation (para. 37 and 68(b)) is a sound idea, although the Report would benefit from more specificity on how and by whom. Strongly support the suggestion that States share good practices and lessons learned on norm implementation (paras. 37 and 68(b)). As a means of facilitating this, endorse the joint proposal of Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa: *National Survey of Implementation of United Nations General Assembly Resolution 70/237.*

**E. Confidence-building Measures**

E1. In general support the content of this section of the Pre-draft as drafted.

E2. The chapeau should reflect consensus text from previous GGE Reports with greater fidelity and clearly distinguish new text. The specific role of the multi-stakeholder community, and the benefits that could be derived by States from this, should be further emphasised (para. 47).

E3. To inform assessment of its merits, welcome further advice on how the proposed global registry of Points of Contacts (PoCs) (para. 68(c)) would be managed, including to avoid duplication of existing regional efforts, but also to capture those States not already included in the existing registries. If retained, the relevant recommendations in the Report should replicate the breadth of PoCs reflected in paragraph 44 of the Pre-draft.

**F. Capacity building**

F1. In general support the content of this section of the Pre-draft as drafted.

F2. Welcome the opportunity to develop – for inclusion in the Report – guiding principles for ICT-related capacity building in the field of international security (para. 68(d)). Paragraph 52 of the Pre-draft, the *Busan Principles* and the *Delhi Communiqué* provide a good starting point for such an effort.

F3. Strongly support the call for greater coordination in capacity building efforts (para. 55). To inform assessment of its merits, further information is required on the nature of the mechanism the Secretary General would establish (para. 68(d)), including how it would be funded and how it would achieve the objective as compared to existing mechanisms such as the Global Forum on Cyber Expertise (GFCE).

F4. Welcome the recommendation that States further cooperate to build capacity – but caution against limiting such cooperation to protection of national, transnational and supranational critical infrastructure (para. 68(d)). Such cooperation should encompass the full breath issues discussed in the capacity building section of the Pre-draft. This recommendation should be expanded to encourage States to mobilise resources in support of such capacity building as well as to encourage integration of cyber capacity building into the larger development agenda of the UN, including the Sustainable Development Goals.

**G. Regular Institutional Dialogue**

G1. Note that at several points the Pre-draft suggests that States hold primary responsibility for maintaining a secure, safe and trustable ICT environment / for national security, public safety and rule of law (e.g. paras. 38 and 65). The Report should acknowledge that, under the UN Charter, States are responsible for *maintaining*

international peace and security, but also re-affirm that all stakeholders have a responsibility to *use* ICTs in a manner that does not endanger international peace and security. We welcome acknowledgement in the Pre-draft of States' unique roles and responsibilities, as well as recognition that there was growing appreciation among delegations that States benefit from the expertise of multi-stakeholder communities and that the responsible behaviour of these communities is essential to the maintenance of peace and security in cyberspace (para. 65).

G2. Australia considers that establishment of a standalone inter-governmental specialised agency (para. 62) is unlikely to receive consensus support at this time. We note proposals made by some delegations for the continuation and/or formalisation of regular institutional dialogue on responsible state behaviour in cyberspace in the context of international security. Should such proposals gain consensus support, such dialogue would most appropriately occur under the auspices of the UN's First Committee. We note the recommendations in the Pre-draft calling for establishment of a new OEWG and a new GGE (para. 68(e)). To inform assessment of the merits of these recommendations, welcome further details on the proposed mandates, commencement, duration, participation and location. In this regard, the existing mandates of the OEWG and GGE, as well as mandates of previous GGEs (especially those endorsed by consensus) may be instructive. Any new dialogue(s) should commence after the conclusion of the current OEWG (July 2020) and GGE (May 2021). A formal mechanism for inclusive multi-stakeholder engagement should be included in any new mandates.

G3. We note the proposal for a Political Binding Instrument/Declaration (para 62). Australia considers that all States have already made a political commitment via UN General Assembly Resolution A/RES/70/237 (which was passed by consensus and which called on all UN Members States 'to be guided in their use of information and communications technologies by the [GGE's] 2015 report'). This political commitment is further reflected in leaders' statements including, but not limited to: *G20 2015; CHOGM 2018; ASEAN Leaders 2018; ASEAN Communications Ministers 2018; EAS Leaders 2018*; and the *Joint Statement on Advancing Responsible State Behaviour in Cyberspace 2019*. Many Member States – including Australia – have also unilaterally and/or bilaterally committed to act in accordance with the 2015 GGE Report. That said, we understand the proposal captured at paragraph 62 of the Pre-draft has broader intent. Should this proposal gain consensus support, the objective of any such Political Declaration on Responsible State Behaviour in Cyberspace should be to elevate the agreed consensus in A/RES/70/237, thereby increasing implementation of, and adherence to, the recommendations in the 2015 GGE Report.

G4. Should a further OEWG/GGE be established (see G2 above), it could provide the forum for States to report on implementation of any Political Declaration (see G3 above) including via a voluntary survey on national implementation, see: joint proposal of

Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa: *National Survey of Implementation of United Nations General Assembly Resolution 70/237.*

**H. Conclusions and Recommendations**

H1. This section of the Pre-draft is unnecessarily duplicative – both of the preceding sections and within the section itself. Specific comments on recommendations are made in the corresponding sections above.

H2. Each individual recommendation that "States continue to inform the Secretary General of their views on [international law/norms/CBMs/capacity building]" (paras. 68 (a)-(d)) should be compressed into one overarching recommendation. A voluntary survey could provide a standardized structure to facilitate this, see: joint proposal of Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa: *National Survey of Implementation of United Nations General Assembly Resolution 70/237.*

H3. Likewise individual recommendations for establishment of various repositories (paras. 68 (a)-(d)) should be combined into one recommendation. To inform assessment of the merits of such a global repository, welcome advice from relevant authorities as to whether such a repository could be incorporated on a cost neutral basis into existing mechanisms (for example: the Secretary General's annual call for updates from States on their use of ICTs in the context of international security, with responses incorporated into existing compilations of responses to that call and/or compiled on UNIDIR's Cyber Policy Portal).

**X. Non-paper listing specific language proposals under agenda item "Rules, Norms and Principles" from written submissions received before 2 March 2020**

X1. Australia welcomes the proactive approach of delegations who submitted specific language to the Chair, as set out in the Non-paper.

X2. While the specific nature, scope and language would require further deliberation (and may not be the subject of consensus), certain proposals may more appropriately be considered in the International Law section of the Report, including for instance:

- China: dot points 1-3 under heading 'State sovereignty in cyberspace'
- Cuba: dot points 1, 6 and 7
- Islamic Republic of Iran: dot points 2-4.

X3. Any language in the Report on the topics above should reflect consensus understanding of the relevant principles of international law, extrapolating their application to State conduct in cyberspace. The Report should also reaffirm that States must comply

with their obligations under international law to respect and protect human rights and fundamental freedoms (ref 28(b) 2015 GGE Report).

X4. While the specific nature, scope and language would require further deliberation (and may not be the subject of consensus), certain proposals may more appropriately be considered in the context of providing guidance for implementation of norms articulated in para 13 of the 2015 GGE report (endorsed by consensus in A/Res/70/237), including:

- China: dot points 1, 3-4 under heading 'Critical infrastructure protection' (ref paras. 13(f) and (g) of the 2015 GGE Report), noting dot point 2 under the same heading appears to duplicate para. 13(f)
- China: dot points 1-3 under heading 'Supply Chain Security' (ref para. 13(i) of the 2015 GGE Report), noting consensus might be found by comparing the current language with the *Prague Proposals* dated 3 May 2019
- Croatia, Finland, France and Slovenia: dot point 2 (ref para. 13(c) of the 2015 GGE Report), noting dot point one appears to duplicate existing para. 13(c) and further noting that relevant language from the *Paris Call* and/or *Global Commission on Stability in Cyberspace* may provide a starting point for further consideration
- Cuba: dot point 2 (ref para. 13(b) of the 2015 GGE Report)
- Islamic Republic of Iran: dot point 5 (ref para. 13(c) of the 2015 UNGGE Report)
- Islamic Republic of Iran: dot point 6 (ref para. 13(i) or (j) of the 2015 UNGGE Report)
- Netherlands: dot points 1-2 (ref para. 13(f) of the 2015 GGE Report), noting that relevant language from the *Paris Call* and/or *Global Commission on Stability in Cyberspace* may provide a starting point for further consideration.

X5. Welcome inclusion in the Report of a new stand-alone norm against cyber-enabled intellectual property theft for commercial gain (ref China: dot point 3, under heading 'Data Security') - provided that the language reflects the *2015 G20 Leaders' Communique*, which has subsequently been endorsed by many countries bilaterally, including by Australia and China (ref *Joint Statement Australia-China High-Level Security Dialogue*, Sydney, 2017).

X6. While not diminishing their importance or gravity, other issues in the Non-paper (including: internet governance, data security and counter-terrorism) would be better addressed in other forums (see: *UNODA Background Paper on existing UN bodies and processes related to the mandate*, available on the OEWG's website).

**Y. General Observations (applicable to all sections above)**

Y1. While preferable for the Report to reflect only consensus reached during discussions, the Report could highlight significant issues about which delegations did not reach consensus and which require further study. However, listing each and every issue raised by delegations may not be constructive. As demonstrated in the Pre-draft, such lists are lengthy and often incomplete. Proposals with little support are presented in the same light as proposals with significant support. If retained, language should be developed to consistently indicate scale of support. This would minimise the risk of misperception by future readers of the Report.

Y2. Encourage consistency of language. As an example, currently "implementation", "operationalisation", and "translation" are used interchangeably. The Report should adopt one term, with its meaning defined in the document. Likewise, "actors" is used throughout the report but with different meanings. Consistent with the OEWG's mandate, the Report should default to "state actors", with substitution (for example, "non-state actors") as appropriate. In a similar vein, the Pre-draft refers variously to "malicious use", "malicious purpose" (etc.). Malicious activity in cyberspace could be interpreted to mean many different things. The Report should adopt language reflective of its mandate, for example: "use of ICTs in a manner inconsistent with international peace and security". For brevity, "malicious activity" could be defined as such early in the report.

Y3. Ensure fidelity of language drawn from existing documents. Text drawn from existing documents should be quoted accurately, with its source acknowledged. Consensus based UN documents, including – but not limited to – GGE Reports and endorsing UNGA resolutions, should not be re-negotiated. References to prior agreement/recognition by the General Assembly should be accompanied by the relevant document references. The Report should clearly demark contextual repetition of agreed consensus text, and new text that that seeks to build upon that consensus.