Position Paper on New Zealand's Participation in the February 2020 Session of the 2019-2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Purpose

This paper aims to support the Chair in his development of a report for the Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. It outlines the major elements of New Zealand's interventions at the second substantive session of February 2020, which the Chair may wish to consider for inclusion in the development of the Group's final report.

Overview

New Zealand reiterates its commitment to the previous consensus decisions of the UN General Assembly to endorse the reports of UNGGEs on Developments in the Field of Information and Telecommunications in the Context of International Security, including with respect to the application of international law online, and the norms of responsible state behaviour online.

New Zealand associates itself with the statements delivered on behalf of the Commonwealth and the Pacific Islands Forum.

New Zealand acknowledges that there is not agreement among the full UN membership as to next steps for increasing cyber stability. It is important that we use this process – and its report – to build trust and confidence among the membership. To this end, we encourage the group to focus on concrete, practical, meaningful and achievable outcomes. We ought to build trust and confidence now, so that we might make progress on more difficult issues in future.

We believe there are clear areas of convergence which can form the basis of any report. In this document, we highlight where we believe those areas may be.

Existing and Potential Threats

We believe that the OEWG's report should take a **technology-neutral** approach, focusing on state behaviour rather than specific technological developments. This ensures our work is enduring – and is not made obsolete by technological developments.

With respect to these behaviours, New Zealand is particularly concerned about, among others, the trend toward malicious compromises of mass personal data; targeted efforts to undermine political systems and elections; the cyber-enabled theft of intellectual property, including from academic and research institutions; and the potential for IOT devices to be utilised by states for malicious purposes.

New Zealand acknowledges the risks presented by cybercrime, and by other online harms, but urges the Group's report to focus on state behaviour online, noting the existence of other avenues – including under UNODC auspices – for international efforts addressing cybercrime.

Norms, Rules and Principles for Responsible State Behaviour

New Zealand thinks that **raising awareness and supporting implementation** of existing norms of responsible state behaviour online as outlined in previous UNGGE reports is one of the most practical and achievable outcomes the OEWG can deliver.

There are different ways in which this awareness-raising and implementation may be carried out:

- We are aware of several countries that have developed written outlines of how they have implemented the norms of responsible state behaviour online. The OEWG's report could encourage other states to do the same.

- We could recommend that regional organisations give consideration to how they may support awareness-raising and implementation of existing norms.

- We could encourage states to ensure norm awareness, understanding and implementation is a feature of cyber security capacity-building programmes.

New Zealand does not rule out elaboration of further norms at some point in the future. At this stage, however, this Group's energy is best focused on achieving progress in areas where we can find consensus, and make practical, meaningful steps forward. On norms, this means focusing, for now, on the implementation of existing commitments.

Cyber stability is not threatened as a result of the absence of norms, or the lack of a framework of responsible state behaviour online. It is threatened because some states are not abiding by the commitments we have all made. To this end, a focus on implementation and a reaffirmation of our intent to abide by our commitments better serves international cyber stability at this stage.

International Law

New Zealand reaffirms its view – and that endorsed by the General Assembly – that international law applies online as it does offline. There are no gaps in international law in cyberspace. Existing international law provides an effective toolkit to regulate state conduct online, identify breaches of international law online, attribute state responsibility for those breaches, and guide responses from victim states.

We acknowledge, however, that there is work to be done to crystallise precisely how existing international law applies online and to secure greater consensus on this

question. New Zealand is giving consideration to sharing our own position, and encourages others to do the same.

We also want to ensure all members are equipped to engage fully in considering how international law applies online. We support calls for a greater focus on international law capacity-building as part of broader cyber security capacity-building efforts. To support us in these efforts we welcome the input and views of civil society, academia and industry.

For the purposes of the report of the OEWG, we therefore support:

- Reaffirmation of the consensus view that international law applies online as it does online;
- Encouraging states to develop and share national views on precisely how international law applies online;
- The development of a repository for such national views, to ensure they are made accessible and to enhance transparency in this field;
- Encouraging states to increase engagement on capacity building as it relates to the application of international law to cyberspace to ensure that all states can meaningfully participate in this discussion.

Confidence-Building Measures

New Zealand sees outcomes on CBMs as one of the most practical and achievable things the OEWG can deliver.

We acknowledge the work on CBMs that has come before by, among others, the OSCE, the ARF and the OSCE, and the CBM recommendations outlined in the report of the 2015 UNGGE.

We are mindful, however, that the regional groups taking forward CBM discussion and implementation do not include the full UN membership. This is a particular concern for New Zealand, including for our close partners in the Pacific. **We need to build trust and confidence across all states.**

It may be that there are certain CBMs which are ripe for universalisation. In doing so, we need to be mindful that CBM discussions in some regional groups are still at a relatively early stage of development. Whatever we do under UN auspices, we need to make sure these groups have the space to continue developing their own practice.

Particular CBMs we may wish to consider implementing at a global level may include:

- A global, voluntary list of cyber security policy points of contact;
- Information-sharing around national cyber security strategies and approaches to incident response;

- Sharing of best-practice crisis-management procedures.

At this stage, we see greater benefit in ensuring current CBMs are delivering effectively, and that their benefits are accruing to all states, rather than looking to create new CBMs. To this end we think we are better off **ensuring existing regional CBMs can be taken up by a broader range of states; operationalising existing commitments, and encouraging best practice CBM implementation; and exercising to ensure CBMs are working effectively**.

We **support the call for the development of a global repository of existing CBMs**. This would inform both regional and global engagement on CBM development.

Capacity-Building

As with CBMs, we believe outcomes on capacity-building would deliver meaningful progress on global cyber stability. We heard this clearly through nearly all interventions during the February session of the OEWG.

We welcome that there is an increased interest in providing cyber security capacity-building, and **encourage further mobilisation** of resource. With increased efforts comes a heightened need to coordinate efforts. We hear this clearly from the partners with which we work on capacity-building.

New Zealand comes to this issue from a particular perspective – that of a capacity-building provider. We do not bear the brunt of the consequences of poor coordination. We welcome the views of those recipients most affected by a lack of coordination in this space.

One of the ways in which we think we can address the issue of coordination is by ensuring donors and recipients are working in partnership on activities. If we are attentive to the needs of our partners – and shaping our support accordingly – we should be less likely to duplicate our efforts.

One way in which we could promote this way of working is through adopting principles of capacity-building, which may include a focus on taking a **partnership approach** (see below).

We also know there are existing mechanisms for coordination, and that these have taken strides in recent years. The GFCE, for example, has achieved a lot in the fewer-than five years it has been in existence. We see these initiatives as having an ongoing important role, and encourage them to continue **to broaden the geographic scope** of their activities – including in the Indo-Pacific.

We think it may be at the **regional level** that activities could be best-coordinated. Regional coordination is potentially more manageable and effective. This group's report

could **recommend such regional coordination, and encourage regional organisations to give effect to it**.

We think the development of principles of capacity-building would be a useful contribution to ensuring global capacity-building efforts are effective. There are existing principles that may be useful to draw on here, including those developed by the GFCE, which highlight inclusivity, ownership, sustainability, trust, transparency and accountability.

New Zealand has its own principles for cyber security capacity building engagement, principles which highlight, among others, partnership, a focus on results and practical outcomes, and a focus on sustainability. It is also important to ensure capacity-building principles take account of the gender dimensions of such work.

Regional Institutional Dialogue

We recognise the benefit that the OEWG has brought. We have appreciated the opportunity to hear from a wide range of member states, to share views and to meet new colleagues. This meeting has in itself been a Confidence Building Measure.

At this stage, we would like the Group's work to crystallise – and the Group's report to be further developed – before we take decisions on any future discussions. Form follows function.

If there is to be further dialogue, we would be interested in this developing according to the following principles:

- Focused on taking forward the OEWG's existing work in practical, tangible ways;
- Established in such a way that is inclusive of small states, and mindful of the resource burden on their systems. Meeting once a year, for a week, for example – rather than anything more regular.
- Reflects the multistakeholder nature of the internet, and includes multistakeholder perspectives;
- Does not duplicate the work of other mechanisms and has a clear focus on international peace and security.

New Zealand regrets that non-ECOSOC accredited organisations were unable to participate in this OEWG session. Discussions on cyber stability should take a multistakeholder approach, reflecting the multistakeholder nature of internet governance and the wide-ranging impact of an unstable and insecure online environment. Any future arrangements should reflect this, and include more multistakeholder voices.