STATEMENT BY THE REPRESENTATIVE OF AUSTRALIA TO THE FIRST SUBSTANTIVE SESSION OF THE OPEN ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS (December 2021)

Norms of responsible State behaviour

It is clear that the international community expects countries to act consistency with their commitments, made in the UN, to the framework of responsible state behaviour in cyberspace, including the 11 norms of responsible state behaviour.

These norms have been developed over time, not imposed top down from the UN, but by collecting together the best practice examples of how countries were addressing cyber threats on the ground.

The report of the 2021 Group of Governmental Experts provides a significant step forward – not only do we have the norms themselves, but also in-depth guidance to all countries on how they can be implemented and applied.

I commend the norms guidance of the 2021 GGE report to all, negotiated and adopted by consensus, and endorsed by consensus in the General Assembly only a few weeks ago.

We heard yesterday and this morning from many States about the significant and increasing threat to critical infrastructure from cyber threats.

Three of our norms provide commitments by us all relevant to critical infrastructure – paraphrasing, these are: protecting our critical infrastructure, refraining from causing damage, and assisting each other in the face of malicious activity targeting critical infrastructure.

In the 2021 OEWG and GGE, and in the face of an unprecedented global health crisis, we saw recognition that medical services and healthcare infrastructure are captured by these norms.

I hope that in our work here we can explore further and advance common understandings of how these norms can protect our health infrastructure from malicious cyber activity.
I use this as an example for one aspect of norms implementation that this group can focus on. I have heard many others put forward by delegations today that may benefit from further discussion.

The logical next step is affecting the imbedding of norms. This requires:

- increased awareness in government and civil society (regional organisations could have positive role);
- increased resources (through capacity building); and
- sharing and availability of best practice (shared understanding of value of norms, and how countries and regions are implementing them).

A core part of implementation of the norms is not only sharing understandings of how to implement them, but to also self-assess what actions each of us have taken to implement the norms, and what actions are still required to implement them fully.

The 2021 OEWG report recommends that states, on a voluntary basis, survey their national efforts to implement the norms.

We have not been idle since that report was adopted – and hope to have an official announcement before our next session in March.

But as an update – Australia is working in close partnership with Mexico and other States to provide an online platform, through the UNIDIR Cyber policy portal, that States can easily use to self-assess progress towards implementation of the consensus recommendations of the 2015 GGE report (UNGA resolution 70/237), with the additional guidance provided in the 2021 OEWG and GGE reports – including norms of responsible state behaviour.

The Survey of national implementation collates national take-up of the recommendations of the 2015 report, with a view to assisting assessment of their further development and implementation.

Surveying implementation through self-assessment provides several benefits: not only can states identify how they have implemented the norms (and I am confident that every country, when they look at their own systems, will see that they have implemented the norms in some capacity), but also where the gaps in implementation may be, and identifying the barriers to implementation, with a view to developing targeted cooperation and capacity
building programmes which might be appropriate to overcome any barriers to implementation or gaps in capacity so identified.

Implementation of the norms is not a once and done thing; it requires review and updating as threats change, technology evolves, and behaviours adapt.

In 2019, Australia published a comprehensive review of how we, across all government agencies, implement the norms. I was struck, when preparing for this new OEWG, by how much has changed in the way Australia implements the norms, and in the way Australia uses the norms to address cyber threats, since 2019.

I take it as homework for Australia to update this review, as a display of our commitment to sharing best practice and national experiences through the survey of national implementation.

Australia also published the results of consultations we held with our private sector, civil society and the technical community to identify cross-sector best practice norms implementation, as part of our contribution to the 2021 GGE – the invaluable input of the multi-stakeholder community to identifying and sharing best practice was tangibly demonstrated in that review, and I’m sure similar input and experience will significantly contribute to our discussions here.

There have been some comments today on the voluntary nature of norms. Australia associates with the comments of Mexico on this issue, and make the following points:

We emphasise the intrinsic interrelation between norms and law.

If norms stood alone – then their voluntary nature might be concerning. But norms don’t stand alone. If we focus primarily on the voluntary nature of norms, we risk missing another significant part of the framework: norms sit alongside international law. Norms are voluntary and non-binding. But the law they sit alongside is binding.

This point is often lost in conversation about voluntary norms.

We have, by consensus, agreed that existing international law – including the UN charter – applies in cyberspace.
Our work here – under our next agenda item – is to elaborate how international law applies.

International law is only effective when it is implemented, adhered to, and enforced. Many have referred in their statements so far to aspects of IL (state sovereignty, non-intervention, refraining from use of force, law of state responsibility, IHL and IHRL).

The path forward is to take the existing frameworks provided by current IL and fill it with deeper, clearer, and more practical understanding of how these rules and principles apply to state behaviour in cyberspace.

And I look forward to continuing that discussion tomorrow.