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)

Existing and Potential Threats

Australia thanks delegations for their nuanced annunciation of some of the threats that are faced in cyberspace – both currently and into the future; and in particular, those who have spoken on the emerging cyber threats to critical healthcare infrastructure, electoral processes, and the damage that ransomware is reaping across all sectors.

I will be brief, and rather than specifying specific threats, make two general points on this part of our agenda, and then take the opportunity to respond to some points that have been made by some delegations.

First -

We are all aware that the cyber threats faced by our global community are significant and growing.

This group is unique – it is the only universal UN forum mandated to explore and address international security issues in cyberspace.

I encourage us all to recognise the significance of this mandate.

This group must focus on those threats which could have serious implications for international peace and security:

- The threats that emanate from the malicious activity of states and their proxies [as mentioned by Indonesia]
- The threats that reach that threshold due, for example, to their scope, severity, and impact increasing the risk of escalation to conflict, and
- The threats unique to the mandate of this group,

without losing sight if the links between our work and that work occurring in other fora across the UN (which I have heard are important to many delegations).

Second -

I would like to emphasise the value in creating a clear link between the existing and emerging threats we identify, and the remainder of our work discussing recommendations and proposals for responsible use of technology – through the application of international law, including international human rights law and international humanitarian law, norms, CBMs and capacity building.

In doing so, Australia considers in important to take into account:

- The human rights impact of certain cyber threats [as Nigeria and Pakistan mentioned]
- The gendered impacts of malicious cyber activity [mentioned by Chile]
- That cyber threats to international peace and security can be context specific: that is, a difference in capacity can impact vulnerability to, and the impact of, malicious cyber activity; and
- That ICTs are not themselves a threat; it is only when they are used inconsistently with international peace and security that they may pose a threat. A technologically neutral approach to recommendations will future-proof our work.

Finally –

A few delegations have raised an issue I would like to take the opportunity to respond to.

Regarding the military development of cyber capabilities, Australia aligns with Denmark's remarks, and particularly the points made about the importance of transparency: transparency breeds accountability, predictability and stability.

Australia emphasises that it is not technologies themselves that are of concern; it is their misuse.

Just as many states are exploring economic development opportunities of these technologies, countries are also exploring military application of these technologies.

Australia is of the view that it is legitimate for states to be exploring these possibilities, provided that this goes hand in hand with acknowledgement that States' activities in cyberspace are guided by same rules as apply to military actions in physical world.

If used responsibly, military cyber tools can have highly discriminate results with limited results on individuals/civilians.

If used responsibility, they can be more discerning then kinetic weapons.

Deepening our understanding of what is responsible behaviour is indeed focus of work we have here.

All military cyber operations must be conducted in accordance with international law and the norms that we have agreed here at the UN.

This includes states' binding UN Charter obligations to peacefully settle disputes and refrain from use of force in international relations.

Australia has spoken publicly to the benefits of international humanitarian law applying in cyberspace. But we should also consider the costs were it not to apply.

Hypothetically, were IHL not to apply, rather than discourage militarisation of cyberspace, it could actually motivate parties to use cyber means and methods of warfare over traditional kinetic weapons.

Faced with significant limits on guns and bombs under IHL, states could place greater reliance on unregulated cyber tools that would achieve the same (or worse) destructive results.

We have differing views on the merits of military cyber capabilities.

The core concern, however, is the misuse of these technologies.

I suggest that to the extent that we consider this issue in existing and emerging threats, it is captured along lines of noting development of these capabilities and expressing concern about their misuse.