Existing and emerging threats

Australia welcomes our discussion today to exchange views on existing and emerging threats to international peace and security in cyberplace.

Thank chair for your summary and questions;

Noting that the summary might serve as helpful aide memoire.

And while not directly referenced in that summary, I note that Australia reads it in the context of our mandate – that is, that we are discussing threats that meet the threshold of impacting international peace and security.

Chair, colleagues,

While we didn’t know the damage that could be caused by ones and zeros when the UN was established in 1946, we certainly know it today.

This global community must be prepared to shine a light on malicious cyber activity and hold the actors responsible to account.

Australia calls on all countries to honour and uphold their commitments to existing international law and norms of responsible state behaviour which apply in cyberspace

Last month, Australia, the United States and the United Kingdom publicly attributed cyber attacks against the Ukrainian banking sector to the Russian Main Intelligence Directorate (GRU).

Cyber-attacks against Ukraine have increased tenfold since Russia’s invasion.

In the lead-up to the invasion, Russia launched cyber-attacks on Ukraine’s banks, denying Ukrainians the ability to use ATMs or transact via their mobile phone apps.

The network takedowns have also inhibited the humanitarian response to assist refugees fleeing war-torn Ukraine.

Let me be clear: this behaviour is unacceptable.

As mentioned by several states here today, the spillover effects of malicious cyber activity can be grave and pose a significant and escalatory threat.

This behaviour is irresponsible, it, creates risks for all states; it poses a grave threat and disruption to international peace and security in cyberspace.
The sophisticated malicious cyber operation on the ICRC discovered earlier this year is yet another example of unacceptable activity in cyberspace. And I thank the representative from the ICRC for her detailed intervention.

And in the interests of time I will simply state that it is of grave concern that a humanitarian organisation - an organisation we have all agreed is neutral, that ought not be targeted, has now been targeted as victim to such an unconscionable attack.

It is not an act that the international community can take lightly, and note the proposal from Switzerland that this group make clear that humanitarian data should not be misused – this deserves further attention from our group.

And makes immediately vital a focus on deepening implementation of the application of the critical infrastructure norms, including to healthcare services.

Further study of the continuously evolving threats that the healthcare sector faces, will help us better understand this threat.

Studying these threats will provide the data and context necessary to effectively respond and increase the overall resilience of the healthcare sector and medical services, particularly in the context of a pandemic.

And I commend the efforts of several partners, including Czech Republic, Microsoft and the Cyberpeace Institute in taking forward this work.

We have also heard the interventions of several delegations today noting that the benefits of digital technologies are not evenly distributed, and the importance of fostering an international community focused upon narrowing the digital divides towards sustainable economic growth, development and stability for all.

The threats that we face are evolving and increasing, but we have a framework, which we have all agreed to, as our collective starting point to address these threats – when it is implemented and adhered to.

the starting point to deliver on an approach to counter such threats is to work on implementing previous agreements –as it relates to all the pillars of our framework – and our framework consists not only of norms, but also existing international law, confidence building measures, all supported by coordinated and effective capacity building.

to do so requires a broad and comprehensive understanding of the threat landscape we face – for which discussions such as this, and advice from experts, prove invaluable.
I very much appreciate the statement from Malaysia in this regard. And the important points made by the Republic of Korea on the importance of cross-sector and cross-border information sharing, including on threats.

I therefore also commend the inputs provided to our discussions thus far by civil society, academia, industry and the technical community – information from all sources is essential to keeping our discussions and our understandings current and relevant.

And the comments made by France on this issue are very helpful. I also hope that we will be able to hear from those experts, throughout our discussions, about what they see across the threat landscape, and I ask the multistakeholder community to share their experience of these cyber threats which threaten critical infrastructure, the health sector, and international peace and security.

And finally, colleagues, I take the opportunity to invite you all to a side event tomorrow lunchtime, hosted by Australia, Mexico, and UNIDIR, to launch the online survey of national implementation of our framework of responsible state behaviour – a tangible measure to implement the recommendations on the 2021 OEWG report. Further details are on the OEWG website, and I can confirm chair that lunch will be provided.

Thank you.