UK STATEMENT - RULES, NORMS AND PRINCIPLES OF RESPONSIBLE BEHAVIOUR

Chair, Indonesia, Vietnam, and Singapore highlighted that ASEAN Member States have been working hard on norm implementation. The UK has worked in partnership with Australia and ASPI and ASEAN Member States to promote development of national pathways to the implementation of norms of responsible state behaviour in cyberspace.

ASPIs contribution to this process which can be found on the stakeholder submission webpage offers participants region-specific perspectives based on real and observed examples of good practice. It is further supported by a GFCE research report which looks at the unique formula each country has taken to implementing the norms.

This work shows that there are many steps to implementing norms, from building awareness and buy-in across government, to assessing implementation strengths and weaknesses, and the taking action domestically. Drawing lessons from ASEAN Member States efforts in this regard would be informative for all OEWG participants as well as inspiring possible similar efforts in other regions.

Chair, we fully support the progress that has been made on the survey explained by Australia and supported by so many States as a tangible step towards working together in this area. We thank them for that.

The activity we are currently seeing emphasises the importance of implementation.

Norm E - respect for human rights - is a current priority. The same rights that people have offline must be protected online. This includes rights such as the applicability of freedom of expression regardless of frontiers and through any media of one’s choice; and the protection of civic space as it extends online and into digital spaces through the right to freedom of peaceful assembly and of association.

We propose a themed discussion in the OEWG of how these rights can be impacted – intentionally or unintentionally – when States make cybersecurity policy. Civil society experts are able to share their expertise of analysing and assessing the impact of cybersecurity policies and propose actions States can take to protect against these impacts.

Finally on Iran’s proposal to agree a final list of norms before proceeding to implementation, we do not consider this to be practical. We do not see a requirement to add to the 11 norms at this time, but we would not agree that new norms would never be needed. The fast paced development of ICTs led to the agreement quoted by our Chinese colleague to consider new norms in the future. We consider this a practical position. We cannot predict the future. We therefore cannot hold back implementation awaiting this unobtainable objective.