UK STATEMENT - CAPACITY BUILDING

Chair, my intervention concerns a contribution that we and others will submit to you in the coming weeks.

In December we highlighted the Oxford Centre Cybersecurity Capacity Maturity Model (CMM) is a first-of-its-kind model to review cybersecurity capacity maturity enabling nations to self-assess, benchmark, better plan investments and national cybersecurity strategies, as well as set priorities for capacity development.

Undergoing a basic needs assessment and developing a national cyber strategy enables States to make the most of international cooperation. This need was recognised in our consensus framework as early as 2013. It is beyond time to make it real.

At least 89 States – including the UK - have taken this first step since 2015 using the CMM. 36 states have gone on to use the process a second time to review their strategy. But that leaves many others who may not have had that opportunity to go through this or a similar process.

Delivery of the CMM is a global effort delivered through a range of well-known stakeholders from the World Bank (with funding from Korea and Japan) to the International Telecommunication Union, and through regional institutions such as the Organization of American States, the Inter-American Development Bank, the Commonwealth Telecommunications Organisation, the Oceania Cyber Security Centre, and the Cybersecurity Capacity Centre for Southern Africa.

We believe that the OEWG provides an opportunity to ensure that all States who wish to work through the CMM or similar model to conduct an initial needs assessment and develop a national strategy, can do so.

We therefore call on all Member States to prioritise their own cybersecurity capacity maturity and recognise the role of these models in enabling international cooperation. By sharing opportunities for best practice we can support practical progress towards identifying States' needs, improving coordination and ensuring that States are appropriately matched to existing opportunities which support international cooperation.

And we call on the OEWG to:

a. Promote the routes by which States can access support – including funding - to conduct the CMM through the above organisations and through the Global Forum for Cyber Expertise (GFCE);
b. Promote alternative routes for those who do not wish to complete a full guided assessment, including the online guides provided by the Oxford GCSCC Centre and the 'national cybersecurity strategy cycle catalogue' available through the GFCE's Cybil Portal; and
c. Invite UNIDIR to track global progress against the movement for States to assess their priority needs and aims and develop national strategies, perhaps through voluntary reporting using the Survey of National Implementation.

Chair undertaking one of these assessments can help States address so many of the challenges raised here this week, including improving the protection of critical national

infrastructure. Such assessments are often implemented by regional organisations – again highlighting their important role.

This contribution is currently co-sponsored by: Australia, Botswana, Chile, Colombia, Dominican Republic Fiji, Georgia, Germany, Iceland, Japan, Malawi, Mauritius, Netherlands, Norway, Peru, Switzerland, Tanzania, Uganda, United Kingdom, and Vanuatu.

The Global Cybersecurity Capacity Centre in Oxford, the Cybersecurity Capacity Centre for Southern Africa (C3SA), the Oceania Cyber Security Centre (OCSC), the Commonwealth Telecommunications Organisation (CTO), the Organisation of American States (OAS), and the Global Forum on Cyber Expertise (GFCE) have also confirmed their support.

Invitation to co-sponsorship is open to all, but particularly the 89 States who have undertaken a CMM, many of whom are in the process of confirming with capitals in the hope of being able to support this contribution.