Chair, The previous OEWG Report laid down the important principles that ‘Capacity-building should … correspond to nationally identified needs and priorities… and be tailored to specific needs and contexts’. We consider the development of national strategies a particularly urgent step as it is only once a State has conducted a basic needs assessment and has an initial national cyber strategy in place that it can truly 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.

We know that at least 87 States – including the UK - have taken this first step since 2015 using the Cybersecurity Capacity Maturity Model (CMM) designed by the Global Cyber Security Capacity Centre in Oxford. 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 through this or a similar process.

The 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. Crucially these are guided assessments where experts can support nations and organisations understand their current situation and how they can make progress in a way that is tailored to their circumstances.

Despite its Oxford home the CMM is a global effort delivered through a range of well-known experts from the World Bank to the International Telecommunication Union (ITU), and through regional institutions such as the Organization of American States, Commonwealth Telecommunications Organisation, the Oceania Cyber Security Centre and the Cybersecurity Capacity Centre for Southern Africa. The adoption of the model by so many diverse organisations demonstrates the positive impact it delivers.

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. To deliver this, we must:

- First, call on all States to take responsibility and recognise the role of these models in enabling international cooperation,
- Secondly, promote the routes by which States can access support – including funding - to conduct the CMM through the organisations already mentioned and through the Global Forum for Cyber Expertise (GFCE),
- Thirdly, where a State has concerns about working through a full guided assessment for any reason, offer alternative routes to reach the same aim – such as the online guides provided by the Oxford Centre and the ‘national cybersecurity strategy cycle catalogue’ available through the GFCE’s
cybilportal which aims to inform countries of the types of support activities available from GFCE Members and Partners, and

- Finally, measure global progress against the movement for States to assess the priority needs and aims, perhaps through voluntary reporting using the Survey of National Implementation.

Chair, the UK believes that practical progress on capacity building should aim to build on and cohere, not duplicate, existing work. We hope this proposal evidences how the OEWG can support the identification of needs, improve coordination and ensure that States are appropriately matched to existing opportunities which support international cooperation.

As already noted, the CMM is a stakeholder developed and implemented model which has in just 6 years led to enormous improvements in States capacity building efforts, and to their ability to cooperate internationally on capacity building and in countering malicious cyber activity. We look forward to the opportunity to hear from the real experts on this topic in future OEWGs.