UK Explanation of Position on the Annual Report of the Open-Ended Working Group, July 2022

The UK extends its thanks to the Chair of the Open-Ended Working Group Ambassador Gafoor, his team, and the working group for all their efforts in this year's discussion and the adoption of our annual progress report by consensus.

This group has taken an historic step in including a clear reference to International Humanitarian Law in this report. The importance of this reference should not be underestimated and we welcome all States flexibility on achieving this outcome, which was important to the UK.

We are pleased to see the group take concrete steps to deliver for Member States in the form of establishing a global Points of Contact Directory. This is an important move forward in binding Member States together in their shared goal of upholding responsible state behaviour in cyberspace.

In addition, the clear roadmap this report puts in place for next year's discussions is crucial if we are to make any kind of progress together. We must go deeper into discussions in order to find elusive consensus on complex issues. That discussion must start now and not wait until we next meet in six months' time.

This is particularly true on capacity building on which we hope to take further steps next time round. We regret that the OEWG was not able to promote practical steps towards building national capacities such as needs assessments and national strategies.

We have joined consensus on this report but note that the OEWG must work to find a balance between providing Member States the support the need to implement the framework of responsible state behaviour and addressing threats to international peace and security in cyberspace, which are real and escalating.

The UK sincerely regrets that the OEWG was unable to fulfil its mandate to promote common understandings of existing threats by commenting on the use of ICTs for military purposes in the Russian war against Ukraine. Resolution 75/240, which created this OEWG, expressed concern "*that a number of States are developing ICT capabilities for military purposes and that the use of such technologies in future conflicts between States is becoming more likely*". This report should have included clear reference to malicious activity that results in cascading critical infrastructure effects in other States with potentially devastating security, economic, social and humanitarian consequences, and noted that technology plays an increasing role in humanitarian work and malicious ICT activity in conflict situations may also disrupt humanitarian operations

With regard to the issue of due diligence, the UK recognises the importance of States taking appropriate, reasonably available, and practicable steps within their capacities to address activities that are acknowledged to be harmful in order to enhance the stability of cyberspace in the interest of all States. But the fact that Framework refers to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace. Discussion of due diligence should remain as part of the Rules, Norms and Principles section of the OEWG.

We further regret that the important contribution of regional organisations to development and implementation of the framework, and the inclusion of stakeholders in the OEWG's programme of work, are diminished. We welcome the contributions of all States, regional

organisations and stakeholders to this process so far. The number of both Member States and stakeholders taking part in these discussions has risen substantially since the start of the First OEWG in September 2019 and we hope we continue to further develop inclusive dialogue in coming sessions.