UN Open-Ended Working Group on developments in ICTs in the context of international security: Commonwealth statement

The UK – in its capacity as Chair-in-Office of the Commonwealth – delivers this statement on behalf of its 54 equal and independent member states.

The Commonwealth welcomes the commencement of the work of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.

In April 2018, the Heads of Government of all 53 Commonwealth nations agreed for the first time a common vision for improving national levels of cyber security competence and increased co-operation. They chose to adopt a Commonwealth Cyber Declaration that reflects Commonwealth values, and sets out a common commitment to a free, open, inclusive and secure cyberspace.

That Declaration is directly relevant to the work we are undertaking here at the UN today and in support of the realisation of the UN Sustainable Development Goals. The 3 pillars of the Declaration: 'A cyberspace that supports economic and social development and rights online'; 'Build the foundations of an effective national cyber security response'; and, particularly, 'Promote stability in cyberspace through international co-operation' serve to guide the approach of all Commonwealth Member States in the field of Information and Communication Technologies in the context of international security.

But more than that, the Declaration supports the notion progressed here in the OEWG that we can still find commonality in our diversity and reach agreement despite our differences. The Declaration underlines that cyberspace provides a common space, within which the diversity and richness of Commonwealth identities can be expressed; and builds on the principles expressed in the 2014 Commonwealth Cyber Governance Model and our shared commitment to Commonwealth values.

Based on those values, and in line with existing international law, despite our diversity as States, all Commonwealth Heads of Government committed to some key tenets that stand us in good stead in this discussion. The most relevant to discussion at the OEWG include:

- recognising the threats to stability in cyberspace and integrity of the critical infrastructure and affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks

- underscoring our shared interest in protecting the security of our networks, security of data, the people that use them, and the services that run on them

- affirming that the same rights that citizens have offline must also be protected online

- noting the importance and involvement of all stakeholders within their respective roles and responsibilities in the good governance of cyberspace

- committing to exploring options to deepen co-operation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures

- committing to take steps towards expanding digital access and digital inclusion for all communities without discrimination and regardless of gender, race, ethnicity, age, geographic location or language

- noting with concern the challenges faced by Commonwealth developing member countries particularly less developed countries and small island developing states and committing to invest in cybersecurity capacity building, including through the transfer of knowledge and technology on mutually agreed terms, the development of skills and training, the promotion of education and research, awareness raising, and access to good practice

- committing to promote frameworks for cyberspace, including the applicability of international law, agreed voluntary norms of responsible state behaviour, and the development and implementation of confidence building measures to encourage trust, co-operation and transparency, consistent with the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International security (UNGGE)

- committing to move forward discussions on how existing international law, including the Charter of the United Nations, and applicable international humanitarian law, applies in cyberspace in all its aspects

Since 2018, every Commonwealth member has taken steps to improve their cyber security competence and capability, and build capacity. A range of pan Commonwealth, regional and national-level activities have resulted in stronger networks to exchange knowledge and expertise, enhanced sharing of

threat intelligence and understanding of risks, and a more informed and engaging civil society. Forty Commonwealth Nations have completed a national cybersecurity capacity review to inform areas of capacity in which their governments might strategically invest in order to become more cyber secure. There are many more examples where countries can demonstrate implementation of the Commonwealth Declaration.

In June 2020, Commonwealth States will meet again at the Heads of Government Meeting in Rwanda and consider how we continue to move forward on this agenda. Our commitment to strengthening the use of information and communication technologies, while enhancing their security, for the purpose of the sustainable development of our societies remains a priority.

All Commonwealth countries are committed to advancing inclusive dialogue in the field of Information and Communication Technologies in the context of international security throughout the upcoming Rwandan period as Chair-in-Office and pledge our full support to these crucial discussions.