[Our shared commitment to law, norms and confidence building in cyberspace](#)

Your Excellencies, Ambassador Lauber, thank you for giving me the floor.

I think I would begin by emphasising an obvious point which is; the world is increasingly digital by default. The choices individual nation-states make about how to develop, apply and regulate digital technology will be consequential for all our countries. And the choices we make together as a 193-strong General Assembly will help shape the development of cyberspace and the nature of peace and security in the 21st century.

Like all good software, the best systems derive from what has been developed and learned in the past. Without sustained agreement on the norms of international relations, peace and security breaks down. As we meet in the Open-Ended Working Group on Cyberspace our discussions can build on two essential ingredients in the United Nations Charter from June 1945. We have a collective commitment to maintain international peace and security, and to promote and respect human rights and fundamental freedoms for all. We also have a shared commitment to uphold international law, which applies in cyberspace just like activities in any other domain. The General Assembly endorsement of this in 2013 and 2015 is an important anchor to help us frame our developing conversation.

And just as good software draws on work done before, the best innovation depends on further embedding what has already been agreed – and working together on emerging issues that matter. No single government working alone can eliminate cyber threats. International cooperation clearly is key. This includes incorporating all stakeholders in the discussion on maintaining a free, open, peaceful and secure cyberspace.

The United Kingdom believes in an open and pluralistic world. We welcome the General Assembly's decisions to create an Open-Ended Working Group (OEWG) and to establish another Group of Government Experts (GGE). We will actively and positively engage with both processes. We are enthusiastic to hear the views of others – Member States who bring diverse perspectives to the table along with other stakeholders who bring insight whether from the private sector, civil society, or academia. We strongly welcome the renewed commitment to hearing from diverse voices in both the OEWG and GGE. The more we listen, the more we learn. The more we learn, the more we can develop the international relations software to sustain international peace and security.

The United Nations General Assembly has already made valuable progress on cyber. Previous Groups of Government Experts have reached helpful consensus reports adopted by the GA. We have agreed an international stability framework for Responsible State Behaviour in cyberspace – based on the application of existing international law, implementation of voluntary norms of responsible state behaviour and confidence building measures. The cumulative value of this work, in particular the 2015 consensus report, which

agreed a set of norms of state behaviour in cyberspace, represents significant steps forward in addressing instability and risk. And the UNGA in 2015 called on all Member States "to be guided in their use of information and communications technologies by the UNGGE's 2015 report".

In addition to leading the U.K. delegation to the OEWG I will also be one of the 25 members of the 2019-21 GGE. We welcome the commitment by the Chairs both processes, Ambassador Lauber and Ambassador Patriota, to coordinate as they pursue their respective mandates.

The United Nations General Assembly has already agreed that international law applies and has agreed a set of voluntary non-binding norms as tools that can strengthen international security by establishing clear expectations for state behaviour in cyberspace. In tandem with Confidence Building Measures (CBMs) these build trust, transparency and security. It is human nature to pay more attention to when international law or norms are being breached than when they are being observed. If international law and norms are mostly observed, those who breach them stand out.

We should also be clear we believe that all States have the legitimate right to develop sovereign cyber capabilities and recognise we have an obligation to ensure they are used in line with existing international law.

The United Kingdom believes in positive action by all States to abide by international law, to implement agreed norms and CBMs, and notes that there is a challenge to make sure that existing norms are better understood, communicated and implemented around the world. Sharing best practices and experience is an ideal way to help achieve this.

Confidence-building measures are one particular theme that the OEWG could productively engage on. This includes drawing on the work of regional groups that has sought to increase the transparency and predictability of state behaviour in cyberspace. Valuable work has been done by the Organisation for Security and Cooperation in Europe (OSCE), the Association of South East Asian Nations (ASEAN) Regional Forum and the Organisation of American States (OAS) in developing and promoting specific CBMs. Another example of this includes the work undertaken across the Commonwealth, where 53 member countries endorsed a cyber-declaration in London in April last year, setting out our shared commitment to law, norms and confidence building in cyberspace.

A number of States and others have commented that there is a real challenge in terms of capacity to address cyber security and implement cyber norms. We agree. This is a high-priority problem and needs addressing. Bilaterally, the United Kingdom is doing its part. We are one of the most active cyber donors in the world, investing over £36m in international cyber work with partners in more than 100 countries across six continents since 2012. We believe that funding international capacity building on cyber is an urgent priority that deserves our collective attention and financial commitment from donors and will look to promote this particular theme in OEWG discussions.

In an increasingly digital world, familiar problems of peace and security

take on a new dimension. Technology brings risks as well as tremendous opportunities. The United Kingdom believes it is important to maintain a balanced and long-term perspective. This Open-Ended Working Group has just fifteen days of discussion and debate in total. We encourage both pragmatism and focus in the process anchored on our collective commitment to make sure the 21st century does not look like the 20th.