Norms – UK statement

Chair, realising the recommendations of previous reports is crucial to progress. We are grateful to those who have bought the national survey mechanism to fruition to help hold States accountable for embedding our framework in their national approaches.

Critical infrastructure protection is a priority. Norm g encourages States to take appropriate measures to protect their critical infrastructure. Since consensus resolutions 58/199 and 64/211 were published on this topic, the principles they contained have been widely developed to support implementation of ‘appropriate measures’. In particular, the focus has been on three core aspects:

- the proper identification by States of their critical infrastructure,
- the existence of national regulatory requirements specific to the cybersecurity of that infrastructure, and
- the implementation of good cybersecurity practice by national CI operators.

As States grow capacity, they implement ‘appropriate measures’ in increasingly sophisticated ways. They may begin with consideration of what constitutes critical infrastructure, but not have a list of these national assets. They may then formalise a list, identifying relevant operators in the process. Updating the list regularly and identifying cross-border dependencies may be the next step and so on. For each of the core aspects there are measurable, identified steps that States can take – this OEWG could focus on promoting progress against some of those steps.

With regard to capacities and structures, we believe a focus on CERTS/CSIRTS and, in particular, incident management processes will promote the realisation of both CNI related norms and norm c (States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs).

To meet this norm, States are required to take appropriate and reasonably available and feasible steps to detect, investigate and
address the situation. These steps may include both the actions a State takes in advance to prepare itself to deal with a relevant incident, as well as the action it takes in response to such an incident occurring. This may include:

- putting in place a system for identifying and categorising national-level incidents,
- establishing a national body for incident response, and
- integrating cybersecurity incident management into national crisis management, both as a factor in its own right and as an element of other crisis scenarios.

Again, we could promote progress here.

But responsible States protect their citizens as well as their infrastructure. The same rights that people have offline must also be protected online. All States must know how to embed human rights into their national approach. The OEWG can assist by ensuring States recognise the role of human rights impact assessments in preparing cybersecurity legislation. And we can ensure States know where to find relevant advice, including on:

- the broader range of relevant rights such as the applicability of freedom of expression regardless of frontiers and through any media of one’s choice; and
- the protection of civic space as it extends online and into digital spaces through the right to freedom of peaceful assembly and of association.

Chair, whilst focusing on implementation the UK remains open to developing new norms over time. Our starting point is that any proposals for new norms must find consensus and not duplicate, rewrite or undercut those that have already been agreed.

Further, we note the Russian call for ‘mandatory rules of the game’.

We wholeheartedly agree that international law - which binds States in their actions - is crucial. That is why multiple reports – including that of the previous OEWG – have affirmed the applicability of existing international law to State’s activity in cyberspace. And it is also the
reason that the General Assembly has adopted all these reports by consensus. So the assertion that there is ‘no existing legal regulation of cyberspace’ is clearly incorrect. In our view it would be a mistake to ignore and undermine the protection provided to all State by existing international law in a rush to write new rules. We look forward to discussing this further under the appropriate section of the mandate.

Chair, the position the UK has shared today has been developed from the extensive contributions of Oxford Global Cybersecurity Capacity Building Centre, and of the Freedom Online Coalition. In doing so the UK aims to deliver on previous recommendations that call for engaging stakeholder voices in policymaking processes.