UK comments on Rev1 of the first annual progress report of the OEWG on security of and in the use of ICTs 2021-2025

Statement delivered on 26 July 2022

Thankyou for the opportunity to speak. I have taken the opportunity of being unable to speak until now to listen carefully to all colleagues.

I extend my thanks to the Chair and his team for their efforts to revise and advance the zero draft in such quick time. These comments build on our contribution on the zero draft.

A roadmap for discussions in the OEWG will allow us to move from general statements to more detailed discussions, which is crucial if we are to make progress together. The UK hopes to achieve that.

But we take this opportunity to reflect that there remain significant differences in this room. We encourage delegations to make full use of their many cyber diplomacy skills in support of the Chair, whilst also managing their own expectations of what we can achieve.

China considers that observation and implementation of our shared, holistic framework is crucial. We agree the report must accurately reflect that. A particular point of concern for us is the vague and inconsistent reference to ICTs – rather than security of and in the use of ICTs, or use of ICTs in the context of international peace and security - throughout the report. This wholly undermines our mandate and changes the nature of the report. We request this be standardised as a priority.

As many have, we also welcome the new language in the introduction on stakeholder modalities, regional organisations and gender. Language referencing the need to ‘strengthen interactions with stakeholders’ should apply throughout the report not to one specific section.

On 7a we add our voice to those countries welcoming the inclusion of this threat context but requesting further additions. The reason we came together at the UN on ICTs in the context of international peace and security was because we judged that ‘the use of ICTs in future conflicts between States is becoming more likely’. It is no longer becoming more likely, it is here. We believe it is possible and valuable to reflect this in our report in a manner that all member States can support. We request the following specific changes in this regard:

At para 1 we support the proposal to include a reference to armed conflict.

At para 7a. We consider this para could include wording related to cascading critical infrastructure effects (as suggested by US), hacktivism and criminal and terrorist activity (Russia), critical infrastructure (Kenya), humanitarian work (Switzerland), the global ICT environment (China) and ransomware (many).

We remain against proposals to address law enforcement activity and mutual legal assistance in this fora. This position has been questioned. We consider that national positions can be legitimately nuanced. We agree that, on occasion, criminal activity including use of ransomware may lead to implications for international peace and
security, thus necessitating discussion in this group. That is different from supporting operational activity on standard law enforcement issues.

At 7b we agree it would be clearer to include these proposals, where they find consensus, under the relevant section of the report. We are content with Australia’s suggestions of how to achieve that. We share the US’s concerns regarding the role of the OEWG and the inclusion of 7biv) and 7bv). Similarly 7bvi) and 7bvii).

As India noted we question whether the wording at 7bv is correct. Our proposal was ‘Cooperation and assistance for encouraging the adoption of secure by design principles and good cyber security risk management practises’ but are happy to discuss.

We recognise data security is a part of the mandate of this group. However we do not accept that discussion of this topic should be expanded to issues such as cross-border data flows or include a call for new standards before we have even discussed the topic.

We support Indonesia’s comments regarding the need to articulate the needs of developing States in building capacity to identify, mitigate and respond to threats. We consider this is the core function of the capacity building section, which currently appears to be overtaken by broader capacity building initiatives to the detriment of progress on our mandate. We would support the inclusion of more language on this topic section F.

On rules, norms and principles, we share US concerns about the language at 8c. Specifically we request deletion of the word innovation. We are unclear what kind of innovation this refers to and how it would fit within the mandate of the OEWG.

We request the correction of language at 8e to reflect the original wording of the 2021 OEWG report. That the perspectives contained the Chairs summary be considered “…in future [UKAdd: UN processes, including in the Open-Ended Working Group] discussion on ICTs within the United Nations.

Finally, we note the proposal at 8a to develop common understandings on technical ICT terms. However we request its deletion from recommendation 2. We are not able to achieve this domestically so will not succeed here.

We share concerns about the approach to allocation of tasks to the Secretariat, including in operational areas and on issues where they will quickly be overwhelmed by volume of input. The report must clarify that any collation of inputs would be from Member State or stakeholder contributions, as appropriate, and within existing resources. This includes at Section D Recommendation 4, and Section E paragraph 10a and Recommendation 3. We also propose to delete Section F recommendation 7 and 8 entirely on this basis.

In closing, I align myself with the statement of the Czech Republic yesterday morning and welcome Russia’s willingness to provide an explanation of its vetoes, preferably to all Member States.