Mr. Chair,

France supports the European Union's statement and would also like to add a few comments in its national capacity.

While all the elements of this Group's mandate are equally important to my delegation, the issue of capacity building is perhaps the most urgent. Our work in this forum, as in previous working groups, allows us to define norms of behavior, to inform and progressively develop their content through our discussions, to adopt recommendations and to guide states in their implementation through exchanges of best practices.

All this is essential. But we also need to ensure that each State has the resources and support to take ownership of these standards and recommendations at the national level, and to implement them effectively. As stated in paragraph 54 of the previous OEWG report, our collective ability to mitigate the effects of malicious ICT activity depends on each state's capacity to prevent and respond appropriately to incidents. Only then can we translate the results of the substantive discussions we are having in this forum into reality.

In the framework of the previous OEWG, France supported the proposal, presented in particular by Australia and Mexico, for a national self-assessment tool (National Implementation Survey of UNGA resolution 70/237) that would allow States to take stock of the progress made, but also to identify the challenges encountered in implementing the norms and recommendations adopted by the international community. As indicated in one of our previous statements, we are pleased that the final report of the previous OEWG recommended to States, in its paragraph 65, to use this tool to report on their national implementation policies.

Mr. Chair, as you know, France, along with 53 other States and the European Union, is promoting the proposal for a Programme of Action (PoA) on cybersecurity, one of the main purposes of which would be to support States in developing their capacities to implement the norms and recommendations agreed upon at the United Nations.

Our ambition would be that this PoA could rely in particular on an analysis of the needs identified by States - for example by using the National Implementation Survey currently under development - to define, identify and support capacity building actions targeted and tailored to these needs. This would result in better enforcement of agreed norms, and thus at the global level, greater network resilience, and greater security and stability in cyberspace. In addition, the States benefiting from these capacity-building actions could develop greater cyber expertise that would allow them to participate even more substantially in the ongoing discussions on cyberspace regulation.

The PoA could also allow for regular monitoring of actions carried out, but also of new threats and new needs that emerge in terms of capacity building, in order to adapt the projects supported accordingly.
In order to carry out these actions, we suggest that the PoA could be provided with specific human and financial resources, which could include the establishment of a dedicated secretariat and a trust fund, which could act as a complement to existing initiatives, some of which have been mentioned by our colleagues. It seems important to us to contribute to the articulation of existing initiatives in order to build together the greatest possible impact.

The PoA would be a permanent and dynamic instrument, which could support the implementation of the agreed normative framework, as well as possible additional norms agreed by consensus in the future, including within this OEWG.

We are open to further discussion on this aspect of our proposal with all interested States. Thank you.