Thank you, Mr. Chair, for giving me the floor.

Let me first address the guiding questions one and two. My delegation would like to stress that this OEWG should focus on building an agile and flexible architecture to create networks or a hub of cooperation for confidence building measures (CBMs). Listening to the presentations from the many delegations, we clearly see that there are variations in CBMs between countries and regions. We believe that linking and harmonizing the variations is the first step for the overall CBMs, and fostering a certain level of technical capacity is prerequisite for the advancement of trust among Member States.

The role of existing, time-tested regional organizations is crucial in developing CBMs given that the gaps are smaller among States of the same region than between regions and that we don’t need to establish any other overlapping and unnecessary platforms. As multi-stakeholders own and operate the vast majority of the cyber infrastructure and are often the primary target of cyberattacks, they possess a number of experiences and ample information to share. During the informal and virtual dialogue with multi-stakeholders on March 24th, many participants were eager to offer help, and some of them even showed their willingness to offer training programs to Member States. By
systematically enlisting the multi-stakeholders from the incipient stage, this OEWG will be able to best engage with regional organizations.

Turning to the guiding question seven, my delegation would like to propose some ways to further utilize the UNIDIR Cyber Policy Portal. After watching the presentation by the UNIDIR Cyber Portal, my delegation is of the view that the Portal has the potential to further broaden its roles in CBMs. Currently the Portal has an extensive database of country profiles. This is information CBMs, similar to the budgets and organizational structures of the militaries of each country. If possible, the Portal can expand its functions to encompass notification, observation, and stabilization CBMs. Notification CBMs can include incident reports of cyberspace. Observation CBMs may pertain to advance warning measures. Stabilization CBMs are similar to crisis management. With the help of multi-stakeholders and CERTs of Member States the Portal will be able to monitor disruptions or malicious activities in cyberspace, issue alert warnings on time, and disseminate system vulnerability reports as well as instructions for remediation.

As for the guiding question ten, my delegation believes that merely sharing point of contacts (POCs) is not sufficient to deal with challenges. Member States should ensure that the POCs are readily available and have enough authorities so that they can respond swiftly and act decisively during a time of crisis. Given the speed of interaction and the complicated nature of disruptions in the cyber world, time and mandates are of essence. We would also like to add that the UNIDIR Cyber Policy Portal can play a repository role for the POCs. Thank you.

###