Thank you, Mr. Chair.

1. At the outset, I wish to congratulate you on your election and to assure you of our full support.

2. The Philippines supports the OEWG’s important role as the inaugural multilateral inclusive intergovernmental body to address comprehensively ICT in the context of international security. We view the process of the OEWG as important in building national capacities and human resource competencies, and in promoting international cooperation, which is the most effective way to address cross-border cybersecurity issues and their complexities.

3. We acknowledge the important strides already achieved by the OEWG. In this regard, we thank Ambassador Lauber of Switzerland for successfully steering the work of the OEWG on the outcome substantive report of which contains important conclusions and recommendations that we should build on. The Philippines was pleased to be part of the consensus on the adoption of the report as it covered a number of our views on critical issues, such as addressing existing and potential threats, the applicability of rules, norms and principles for responsible state behavior, our common understanding of international law in the subject of cybersecurity, and best practices in confidence-building measures, capacity-building, and regular institutional dialogue.

4. The National Cybersecurity Plan of the Philippines mandates securing critical ICT infrastructure while ensuring personal data privacy and confidentiality. It is important that
our information infrastructure, or “infostructure,” is resilient, robust, and secure against cyberthreats. Within this framework, I wish to highlight our positions on some of the agenda issues before us:

- With increased dependence on ICTs in providing vital governmental services, disseminating essential information and improving commerce and healthcare systems, we should continue to **build resilience against existing and potential threats** to our privacy and security. Malicious activities in cyberspace are not only designed to attack individuals, but also aim to impair both national critical infrastructure and critical information infrastructure that support delivery of these services to the public.

- We continue to underscore the importance of the **application of international law** and the **UN Charter** which govern the actions and relations between States, and on the 11 voluntary, non-binding **norms** which provide additional guidance on the standard of the international community of what constitutes responsible State behavior in cyberspace. Developing further rules of behavior in cyberspace will contribute to **confidence building** by increasing transparency and cooperation between States and for reducing the risk of conflict.

- Developing countries such as the Philippines count on **capacity-building** as an enabler for all States to contribute to increased stability and security globally. Such capacity-building efforts must be sustainable, evidence-based, demand-driven, politically-neutral, transparent and accountable. It must also respect human rights and fundamental freedoms, be gender sensitive and inclusive, and universal and non-discriminatory.

- To facilitate robust and inclusive discussions, we hope that the **regular institutional dialogue** that we establish through this OEWG will provide opportunities to further develop and operationalize our global framework of cooperative measures to address cybersecurity threats. In this respect, we envision advancing common understandings, exchanging lessons learned and good practices in implementation, building confidence and increasing capacity amongst States.

Mr. Chair,

In this time of uncertainty, States as well as the private sector, scientists and other actors, have leveraged and continue to leverage digital technology to keep individuals and societies connected and healthy. The pandemic and the corresponding life adjustments we have had to make have dramatically increased the value of cyberspace and internet connectivity in our lives. More than ever, our discussions in this working group will be most relevant and far-reaching.

Thank you.

* * *