Let me address the third guiding question first: how we can fill any gaps in the framework? I would first like to mention the process of norm-making. The current 11 agreed norms were made by independent experts, and then later endorsed by the General Assembly. In terms of rule-making in the area of both technical and political nature, I found this process to be most appropriate. For that very reason, however, we have to ask whether this OEWG setting can make comparable achievement. Furthermore, we are aware that the last GGE failed to make further progress. So, our advice is prudence against the creation of new norms, unless we face a manifest gap and compelling reasons to fill such a gap. Thus, the priority should be placed on the elaboration and clarification of the 11 norms, as the Netherlands explained well at the first session.

This leads me to guiding question four: Are there any rules, norms, and principles which can currently be further elaborated in specific ways? When reviewing the current norms, my delegation tries to put one question in mind: whether, and to what extent, the norm is useful and effective in protecting any potential and real victim States; many of which are exposed but less equipped with technical capacity, in other words, how the afflicted States can make use of this norm in seeking cooperation from other States.

My delegation would like to suggest, in this regard, that the current agreed framework can be elaborated in a way that an affected State can take procedural steps to seek cooperation, and other States offer such cooperation.
We thus support the initiative of developing a guidance or guideline on norms implementation in this direction.

Many of our agreed norms are pertinent to the so-called due diligence. The Republic of Korea has proposed a set of procedural steps to take in case a State finds itself a target or victim of cyberattacks. We are willing to suggest and discuss the details of such a procedural approach. In this regard, my delegation wishes to underline that this duty of due diligence is getting increasingly important in both preventing and responding to cyber incidents. Sovereignty has another side of coin, the duty not to allow it to be used for harming another’s sovereignty.

Turning now to the first guiding question with regard to the specific actions we can take. My delegation believes that wider participation of the national survey of implementation, proposed by Australia and Mexico, would be the first step in the right direction as a basis of knowledge and it can also serve as a tool for internal-checking. We also support the exchange of national implementation of the agreed normative framework. The Republic of Korea found the entire experience of internally drawing up the implementation paper to be instructive and helpful in terms of coordinating and integrating relevant agencies under this normative framework.

On a broader perspective, we can get some ideas, for instance, from international civil aviation such as the information-sharing system among governments and industry, the way standards and recommended practices are distinguished, and the mechanism of helping States better comply with those norms with practical and procedural guidance, in order to enhance the safety
and security of air navigation.

One obvious caveat would be that the traditional triangular roles of governments to regulate, industry to be regulated, and consumers to be protected are not clear-cut in cyberspace. In this sense, too, multi-stakeholders’ participation is critical for our efforts.

Lastly, my delegation agrees with the Chair’s approach that the OEWG does not have to wait until the end to forge some progress. We can operationalize what we can do at this stage and build momentum. The proposals of a national survey and a repository of national implementation, I believe, are those we can begin doing at an early stage.

Thank you. /END/