At the outset, my delegation joins alongside the international community and reiterates the Korean Government’s strong condemnation of Russia’s armed invasion of Ukraine. The previous session of last December underscored the importance of implementing norms and international law. Equally important is our resolve to call out, loudly and collectively, any violation of the norms and laws. Only by doing so, we can make this discussion meaningful and strengthen compliance rather than condoning deviation.

Let me address your first guiding question: what preventive and responsive measures can States consider implementing in response to the potential threats? This question is intended to encourage us to pursue some concrete measures instead of merely listing or updating threats. I agree with the need to establish some coherent linkages between this agenda of threats and the rest of our agendas with regard to tangible responses.

However, my delegation is not so sure about whether we are ready at this stage, and under this format, to engage in designing and adopting specific measures, for instance, against ransomware or AI-based incidents. Instead, this OEWG should focus more on building an architecture which is both agile and flexible enough to respond to potential threats. This architecture could take the shape of cooperative networks or a hub of cooperation for CBM, capacity-building, and implementation; but not that of a rule-making body or control
Turning to another guiding question: How can States work together to share new information on existing and potential threats in real-time? Information-sharing is instrumental in prevention, response, and recovery. Yet we first have to work out: sharing with whom, how, and what data? This can be simple warnings, technical, context-specific, sensitive, inter-State only or both public and private. Korea, for instance, has restructured its info-sharing platform, “Cyber Threat Analysis and Sharing,” from a closed platform to an open platform for all interested companies. And trust is thus a prerequisite to any sufficiently useful info-sharing arrangement.

Taking this into account, our option could be to merge and expand already existing info-sharing systems from regional to cross-regional and global, taking also into account national best practices. But this should be best done based on the inputs of experts to ensure technical effectiveness while avoiding any overlap with preexisting working arrangements, for instance, among CERTS.

These questions ultimately concern what kind of objectives and improvements we should pursue, and how to do it. My delegation believes that our way forward should be incremental to build trust and based on the input of experts to ensure we are technically sound. Thus, our immediate focus should be to make use of existing mechanisms, to link regional initiatives, to transplant a workable framework into our own, and to work with the private sector and civil society organizations in partnership.
We also need to have a deeper interface between policy-makers and experts, and do more to synergize multi-layered cooperation at technical, policy, law-enforcement, and strategic levels. It might sound like a patchwork, but that's what cyberspace is, open and decentralized, and we should manage our expectations and pursue realistic goals.

One last point I would like to mention with regard to threat is the human element. I believe we often overlook the fact that cybersecurity's most persistent threat and vulnerability is human behavior. Many of the most critical incidents often turn out to be a consequence of human negligence. This point is something we need to bear in mind when we discuss and design confidence-building measures and capacity-building moving forward.

Thank you. /END/