Thank you, Mr Chair, for continuous inclusive stakeholder engagement. I am honored to be here.

First, new emerging technologies such as AI and quantum computing can be used positively or negatively. We need threat measures and risk assessments based on human live impacts. For practical implementation against supply chain and ransomware attacks, Stakeholders can contribute protection solutions and tools working with States addressing the critical infrastructure by product and sector, addressing threat life-cycle including back-door detection, data integrity, emergency response, remediation, and improvements.

Second, the draft Checklist with 11 norms is comprehensive and actionable to start with. Additional norm to consider includes continuous technology impacts to humanitarian risks regardless of the peace or war time, in such sectors as healthcare, energy, and water. Thank you, a group of 13 countries for sharing Working Paper on Application of international humanitarian law on March 1st to clarify IHL position further.

Third, another suggestion on norm checklist is to clarify capacity building, spelling out 1) timely disclosure vs. remediation, since automated threats can exploit right after disclosure, related with Norm I and J, 2) coordination with regulations and compliance beyond jurisdictions through international standards and certifications in Norm I.

Fourth, about capacity building, the best practice to protect critical infrastructure include Security-by-design and default, Zero-Trust architecture in every component of digitized supply chain from end-to-end, including Hardware, Software, Firmware, IoT, Chips, Cloud, Data, Human in the loop, Suppliers including small & medium, and customers and citizens.

Finally, public-private collaborations, Global Roundtable is a great step up. Peace, safe, and resilient environment can be accomplished by working together with trust, supplemented by positive use of technologies for civilization.

Thank you, Mr Chair!