Good afternoon, Mr Chair, and esteemed Delegates,

My name is Talita Dias and today I am speaking on behalf of the Oxford Institute for Ethics, Law and Armed Conflict (‘ELAC’). As requested by the Chair, my remarks will focus on ‘how Member States and stakeholders can better coordinate and cooperate in the area of capacity-building’. This intervention builds on the work that my team and I have conducted on the application and implementation of international law in cyberspace, including in the context of the so-called Oxford Process on International Law Protections in Cyberspace. This is an ongoing research project that seeks to respond to critical cyber threats by clarifying how different rules of international law safeguard some of the most vulnerable targets of malicious cyber operations, including the health care sector and electoral processes, against the most significant means of attack, such as information operations and ransomware.

First and foremost, we wish to reiterate not only that international law applies to information and communications technologies (ICTs), as previously affirmed in the OEWG and GGE reports, but also that international law applies in its entirety to those technologies.

Secondly, and most crucially, some existing rules of international law applicable to ICTs require member states to build the necessary capacity to prevent, halt and redress a number of online harms. Most notably, while general obligations requiring states to exercise due care or due diligence online and offline, such as the no-harm principle, are obligations of conduct requiring states to do what they can to prevent or mitigate certain harms or risks, lack of capacity is no excuse for inaction. This is because such protective duties have a capacity-building component that require states to put in place the minimal governmental infrastructure enabling them to fulfil such duties of care. The same is true of states’ positive human rights obligations, that is, obligations to protect individual human rights from physical or non-physical threats as well as to ensure their full enjoyment online and offline. Companies should also exercise due diligence to mitigate their human rights impact online and offline, in line with their human rights responsibilities.

This minimal state obligation to build capacity, entails, in the first place, legal capacity-building, that is, acquiring the necessary knowledge of how states’ international obligations apply to ICTs. As an academic institute focused on legal and policy research, ELAC has offered states and other stakeholders the opportunity to acquire such legal capacity or know-how through various means. For instance, in our periodic workshops that have so far led to the...
Five Oxford Statements on International Law Protections in Cyberspace, we have invited and continue to invite and encourage the active participation of representatives of states, international organisations, the industry and civil society groups. We have also partnered with institutions that have sought to benefit from our work, such as the Organization of American States, by offering tailored legal capacity-building workshops and courses. We would like to invite other interested stakeholders to do the same, stressing that we are open to engaging in similar legal capacity-building initiatives.

Thirdly, and finally, we would like to stress that knowing the law is not enough for states to discharge their various capacity-building duties. The actual implementation of basic protective measures in the ICT environment is key. These include the enactment of basic cyber and information security regulations, the establishment of computer emergency response teams and open channels of communication and cooperation with other states and relevant stakeholders.

We look forward to our continued participation in the OEWG.

Thank you.