Intervention by the EU Institute for Security Studies

6th meeting of the OEWG

27 July 2022

First set of questions

Thank you for the opportunity to contribute to this discussion.

For the sake of time, I will keep my intervention brief. We will provide a more detailed written submission on the draft progress report to the Secretariat.

Acknowledging that the discussion on the draft progress report is already quite advanced and many concrete recommendations and comments were already made by national delegations, I would like to focus on two main points: one general and one substantive. Our substantive point is a recommendation that the OEWG starts working on the list of concrete "Cyber Capacity Goals" (CCGs) to be achieved by the international community by 2030.

Regarding **the general point:** we share the assessment of those delegations that expressed scepticism about the Secretariat's operational capacities and the OEWG mandate to deliver on the recommendations in the section devoted to capacity building.

The report on "International Cyber Capacity Building: Global Trends and Scenarios" that the EUISS published last year clearly pointed out the need for all organisations in the cyber capacity building community to prepare for the continued growth of the field. Therefore, in our view, this is not the time for experimentation, but rather the time to focus on delivery.

As the field continues to grow, coordination will become ever more important. Better coordination could be achieved by organisations improving their internal information sharing, supporting processes for international coordination such as the GFCE, and making better use of in-country coordination efforts in partnership with host governments.

Now to my substantive point. Given the importance of cyber capacity building for the debate about design and implementation of norms, confidence-building measures, international law and societal resilience, we propose that the OEWG put forward a list of concrete "Cyber Capacity Goals" (CCGs) to be achieved by the international community by 2030. The starting point for such a list could be the list contained in the 2015 GGE report and other elements identified by the cyber capacity building community, such as adopting a national cyber security framework or establishing a CERT.

Such goals could also help identify which parts of the UN system are best suited to support these objectives, including the role of lending institutions such as the World Bank and development agencies like UNDP. Such approach would also help to reconcile differences in priorities and needs identified by States and their commitments at the international level.

Therefore, we would like to make the following recommendation:

States are invited, on a voluntary basis, to work together with relevant stakeholders, including regional organisations, businesses, non-governmental organisations, and academia, to propose a catalogue of concrete Cyber Capacity Goals (CCGs) to be achieved by the international community by 2030 with the aim to support States in meeting their commitments and exercising their rights resulting from the consecutive reports of the Group of Governmental Experts and OEWG reports.

I understand that this concrete recommendation may be difficult to integrate in the report at this stage. Therefore, I would like to request that this topic is addressed during the subsequent sessions of the OEWG.

We will also share with the secretariat the report on global trends and scenarios in cyber capacity building that I have mentioned earlier.

Thank you, Mr Chair.