First session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

New York, 28.2.-11.3.2022

Agenda item 3: General debate

Statement by Finland

Tuesday, 1 March 2022

Madam Chair,

Finland fully aligns itself with the EU statement, and with many of the remarks already heard in this room. I would still like to deliver a few additional remarks in our national capacity.

I would like to take the opportunity to thank you and the Secretariat for your tireless efforts to organize this meeting under these challenging circumstances. I assure you of my delegation's willingness to engage constructively in this process.

Madam Chair,

With cybercrime becoming increasingly wide-spread, rapidly sophisticated and affecting daily lives of our citizens, there is an acute need for the international community to redouble its efforts to counter cybercrime. The critical functions of society and the daily lives of our citizens are becoming increasingly dependent on information and telecommunications technology. Hence cybersecurity and thereby also our ability to counter cybercrime globally bears profound implications for advancing the prosperity and the well-being of our societies and more broadly for promoting international peace and security, as well as sustainable development. In the interconnected cyber domain, security challenges affect us all and no single country can effectively tackle them on its own.

Our shared goal and efforts to meaningfully work towards a future UN convention to counter cybercrime have, however, been seriously undermined by the current circumstances we are facing due to the grave situation unfolding in Ukraine.

We condemn, in the strongest possible terms, the unprovoked invasion of Ukraine by the armed forces of the Russian Federation. Finland firmly supports Ukraine's independence, sovereignty, self-determination and territorial integrity. Russia must cease military operations immediately. The Russian aggression is causing immense suffering for the Ukrainians. Civilians have died; many more have had to flee their homes. There is no justification for this. It is a flagrant violation of international law, the UN Charter, and the core principles of the international rules-based order. This act of aggression undercuts the role of various relevant UN processes, such as this one, to bring peace and stability to cyberspace and beyond.

Madam Chair,

As for a future UN convention on cybercrime, I wish to underscore the key aspects that should serve as starting points for our deliberations.

Firstly, this endeavor must be guided by rigorous adherence to international human rights norms and standards, with emphasis on the need to protect the victims of cybercrime.

Any substantive provisions in a future UN convention must be clearly defined, and be fully compatible with international human rights standards and our shared objective to build a global, open, free, stable and secure cyberspace. Vague provisions criminalizing behaviour that is not clearly defined in a future UN Convention would risk interfering with human rights and fundamental freedoms and thus must be avoided.

Secondly, my delegation is firmly of the view that the scope of a future UN Convention should be focused primarily on substantive criminal and criminal procedural law and necessary mechanisms for promoting international cooperation. In order to attain its primary objectives and intended effect of countering cybercrime, a future UN instrument should define precisely the terms it employs and be based on the pertinent concepts in existing international texts.

The provisions to be included in a future UN convention or instrument should thus relate only to high-tech crimes and cyber-dependent crime, such as illegally gaining access to, intercepting or interfering with computer data and systems.

Madam Chair,

The need for global capacity building efforts has been aptly highlighted by the GGE and OEWG. International cooperation in cyber capacity building can strengthen States' ability to detect, investigate and respond in a timely and effective fashion to various threats emanating from cyberspace. This should be duly taken into consideration in the work of this Committee.

There is also a clear need for a further, broad-based dialogue between relevant stakeholders in order to foster better understanding of the opportunities and challenges related to global capacity building. Talks and cooperation between States are necessary, but not sufficient. Ensuring a free, open and secure cyberspace where fundamental freedoms are guaranteed, is not only in our common interest but also our shared responsibility. We need to reach out and listen to all interested stakeholders of cyberspace – the private sector, civil society and academia. We expect this Committee to provide a useful contribution to the global capacity building efforts.

In closing, we are looking forward to a constructive process.

I thank you Madam Chair.