Statement by Estonia at the first substantive session of the 2021-2025 UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Discussion under agenda item 5 in relation to international law, 16 December 2021

Thank you, Mr Chair, for giving me the floor.

Estonia sees existing international law as the heart and soul of the framework for responsible state behaviour in cyberspace. We are encouraged that a great many delegations have also stressed that the new OEWG should dedicate itself to continuing to study how international law applies to state use of ICTs, together with the other pillars of the framework.

It is our firm opinion that all states, both big and small, benefit from rights provided by international law - provided that obligations deriving from it are followed. There is a uniqueness to cyberspace, but when discussing how bodies of international law apply, this uniqueness must not be seen as a restriction to the application of these bodies of law – such as the UN Charter in its entirety, the law of state responsibility, international humanitarian law or international human rights law.

We as the international community already have had success in agreeing upon substantial positions regarding international law thanks to efforts in the GGEs. We clearly align ourselves with those delegations who have emphasised and explained that the next step of the international community is to further understand how existing international law applies. We have not had this substantial discussion yet and need to make the best use of the opportunity provided by this group. Therefore, this new OEWG offers us the chance to have a deeper discussion on how these provisions apply in practice, in order to advance common understandings.

Estonia welcomes the efforts by many states presenting their views on these matters. We have published our positions on how international law applies in cyberspace on several occasions. It has been especially positive to hear that many states are continuing their work to publish their positions for the first time or further elaborate on what they have presented thus far.

A number of delegations have also expressed that international law must stay technologically neutral. Estonia agrees with this wholeheartedly and notes that it can and must be applied also to new areas and new attributes of state conduct, including State use of ICTs.

This brings me to the issue of capacity building. During the first OEWG, it was made clear that international law should become an integral part of the capacity
building projects and efforts. This was also stressed in the GGE consensus report agreed only a few months later.

As we take our discussions on international law further, it should be done hand in hand with initiatives that provide a forum for discussions in settings that inspire trust and involve also the multistakeholder community, including academia. Workshops are a welcome example, including at regional level. For example, only last week Estonia, together with the International Committee of the Red Cross and other partners, hosted a scenario-based workshop for a group of countries from Central and Eastern Europe, allowing us to have a rather substantive exchange of views on matters of international humanitarian law.

More States could make use of scenario-based initiatives that could further help to facilitate capacity building efforts. For example, we draw attention to the initiative called the Cyber Law Toolkit. This is a dynamic interactive web-based resource for legal professionals who work with matters at the intersection of international law and cyber operations.

Another initiative we would like to highlight is the recently launched Tallinn Manual 3.0 project, an independent and much renowned research initiative. This new process will revise and expand the Tallinn Manual 2.0 edition, in light of State practice and official statements on the applicability of international law to cyber operations. The activities of international fora, academic scholarship, and multistakeholder initiatives will also be considered and experts around the world are invited to present their contributions.

Mr Chair,

The UNIDIR Cyber Policy Portal has proven a useful platform where states can have quick and timely access to best practices shared by states. Given the length of the current OEWG, this platform should find even wider endorsement and use by Member States as a knowledge hub and transparency measure. It offers an additional platform to share as well as study positions on international law. In addition, the OEWG could encourage additional informal workshops together with multi-stakeholder partners.

Mr Chair,

As for the specific rules and principles that the group should address, we believe that this should be based on what the GGE consensus reports and the OEWG consensus report already include as well as what has been brought forward repeatedly by delegations during meetings as regards to the provisions of existing international law.
For example, there is scope to further look at the law of state responsibility. We could substantiate these discussions by also considering the responsive measures that international law foresees when internationally wrongful cyber operations are conducted — these include retorsions, countermeasures, necessity and the right to self-defence.

Furthermore, Estonia finds that two of the main areas of international law that need to be addressed in this group, given its broad aim to ensure international peace and security, are international human rights law and international humanitarian law.

Firstly, it is critical that human rights and fundamental freedoms are ensured online as they are offline. As mentioned by many during our discussions on risks, there are an increasing number of threats to human rights stemming from the malicious use of cyberspace.

The obligation to ensure human rights and fundamental freedoms is the one of the key duties of states. Cybersecurity and human rights are complementary, therefore must be pursued together to effectively promote freedom and security. National cybersecurity laws, policies and practices must not be used as a pretext to restrict human rights and fundamental freedoms.

The prevention, mitigation of as well as responses to cyber incidents must not violate human rights. This in particular includes the freedom of expression, the freedom to seek, receive and impart information, the freedom to peaceful assembly and association, and the right to privacy.

Secondly, the latest GGE consensus report explicitly mentioned international humanitarian law and recommended the further study of IHL principles. Armed conflicts today and in the future may involve offensive cyber capabilities. Estonia stresses that the use of such capabilities must be subject to obligations deriving from international humanitarian law, taking into account the four IHL principles noted in the 2015 GGE report.

Given the protective nature of IHL, in our view it does not seem representative to assume a link between militarisation and IHL. Rather, it is the other way around. Leaving cyberspace outside the scope of IHL rules would leave civilians, civilian infrastructure and combatants without an additional layer of protections. In the instance of armed conflict, IHL is vital to reduce humanitarian harm.

From our point of view, these are the key international law areas that should be further studied in relation to new technologies to create common understandings on how they apply given the attributes of state use of ICTs. Of course, understanding on how international law applies may differ — after all, put four
lawyers in the room and there will always be at least five opinions. However, we have the timely opportunity to seek ways towards converging views in more areas of international law, step by step.

Thank you, Mr Chair.