Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, February 10 and 11

Mr Chair,

Finland is convinced that a rules-based international order it is our best hope in tackling present and future global challenges, including in cyberspace.

We have been very pleased with the work of the OEWG so far. The engagement of the whole of the UN membership is vital in securing free, open and secure cyberspace.

We also see merit in processes that allow for broad and inclusive participation, including by interested non-state actors, such as business, NGOs and academia. Like Mexico, Switzerland and Canada we regret that the participation of observers in the OEWG was limited to those accredited in the ECOSOC.

Rules, norms and principles

Finland considers that the rules, norms and principles of responsible State behavior are essential elements in building and maintaining free, open and secure cyberspace.

The rules, norms and principles of responsible State behavior that have already been agreed upon should not be reopened. However, there are areas where further refinement and concretization in the interest of their effective implementation seems possible and would be useful.

Additional voluntary cyber-specific norms of responsible State behavior could also be formulated, provided that such norms respond to a clear need and are well argued and formulated. The ones mentioned by the Netherlands, i.e. the protection of the public core of the Internet and the protection of the democratic processes seem to fall into that category.

However, the OEWG must make sure that what is stated is consistent with international law and does not create confusion. Of course, any voluntary norms, rules and principles – whether already agreed or new - are without prejudice to States' rights and obligations under international law. We would support including

in the report of the OEWG a general clause stating that nothing in the work of the OEWG should be interpreted as undermining international law.

We do not see for the time being a need for a new international instrument for cyber issues. It would be more useful to focus on reaffirming and clarifying existing rules and principles.

It is important to raise awareness of existing norms and commitments. The report of the OEWG should be made as clear and as accessible as possible so that it would be useful as further guidance to states.

The regular institutional dialogue, again, would play an important role in strengthening the implementation of the voluntary norms, rules and principles that we have agreed on.

Mr Chair,

We spoke yesterday on Rules norms and principles of responsible State behavior, which are closely linked to international law.

This time we would offer some further comments on international law and try to respond to some of the questions presented in the very helpful paper you prepared for us.

As the applicability of international law to State conduct in cyberspace is now widely recognized, in line with the 2013 and 2015 consensus reports of the GGE, we would not be keen to speak about "gaps" in law as such. Of course, there are areas, where discussions are necessary and ongoing on *how* international law applies to State use of ICTs. This is true, for instance, regarding certain provisions of international humanitarian law. The OEWG could draw on those debates and the very helpful ICRC contribution to this body.

Finland believes that international cyber stability is firmly rooted in existing international law. It goes without saying that this includes the Charter of the United Nations, international humanitarian law and human rights law, which are of particular relevance from the point of view of the mandate of the OEWG.

Human rights and fundamental freedoms as enshrined in the relevant international instruments must be respected and upheld equally online/offline. A number of

specific human rights such as the freedom of opinion and expression, including the right to access to information, and the right to privacy are particularly relevant in cyberspace. Furthermore, each State has to protect individuals within its territory and subject to its jurisdiction from interference with their rights by third parties.

At this juncture I would like to refer to the recently issued statement by the Freedom Online Coalition (FOC) on the human rights impact of cybersecurity laws, policies and practices. Finland fully supports the new statement and is pleased to assume the Chairmanship of the coalition next year.

While the existing international law applies in cyberspace, the application of certain provisions may give rise to practical problems due to the specific characteristics of cyberspace. We feel that it is time to move forward to discuss operationalization of international law in the ICT environment. More clarity would indeed be welcome in some areas, such as International humanitarian law and State responsibility.

International humanitarian law only applies to cyber operations when such operations are part of, or amount to, an armed conflict. At the same time, when cyber operations are launched in the context of a pre-existing armed conflict, there is no reason to deny the need for the protections that international humanitarian law provides.

From this follows that cyber means and methods of warfare must comply with the principles of distinction, proportionality and precautions, as well as the specific rules flowing from these principles.

The unique characteristics of cyberspace, such as interconnectedness and anonymity, affect the interpretation and application of international humanitarian law with regard to cyber warfare. The related problems can nevertheless mostly be solved on the basis of existing rules.

We find due diligence particularly pertinent in the cyber environment. It is clear that States have an obligation not to knowingly allow their territory to be used for activities that cause serious harm to other States, whether using ICTs or otherwise.

If harmful cyber activity takes place and causes serious harm to another State, the State of origin must take appropriate action to terminate it, as well as to investigate the incident and bring those responsible to justice.

It should be recalled that due diligence is an obligation of conduct, not one of result. In general, what is required of States is that they take all measures that are feasible under the circumstances. While States must show due diligence in the control of the national territory, doing so does not release them from the observance of other international obligations such as those relating to human rights.

Some states have recently made known their positions regarding how international law applies in cyberspace. We find these pronouncements helpful, also in the sense that they probably help States to have more informed views on how international law applies in cyberspace. We are currently working on our own articulation on this topic.