Informal inputs to the intersessional meeting of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security

I will be responding to the framing question, “what are the most significant cyber threats”, and in that regard want to highlight three points:

1. All of the tactics or methodologies, or “means or methods” of cyber warfare that we are talking about today are significant and problematic. And more than that, they are also rapidly evolving and changing. Moreover, states also have different cyber security concerns and priorities – it is not an even landscape.
   - So rather than wanting to pinpoint a specific activity or technology under this topic of threats, we would like to stress instead the threat to peace posed by the wider transition by states and their proxies to using ICTs as a tool of or medium for, violence. The is becoming more regular and, as a result, normalised by a larger number of states, and really, without question or debate. The militarisation of cyber space is in progress and not being challenged so much as permitted with some damage control or limitation.
   - To that end, we would suggest that while respecting the importance, and necessity, of reality-based dialogue about specific technological threats, it will also be important to continue focusing dialogue on behaviour and actions. Technology will always be evolving and ahead of law.

2. A second threat to highlight are those to human rights and freedoms, and the human cost of cyber operations. The human cost of attacks on critical infrastructure should be at the centre of how we understand and respond to threats. When defining the components of critical infrastructure—a matter that deserves greater attention and the establishment of a universal understanding—the human impact should take a more prominent and explicit role in that dialogue than it has to date. At the same time, the cyber security-related laws, policies and practices should not be used as a pretext to violate human rights. Some states have expressed reservations about incorporating this perspective in this forum, but there is precedent from other issues and topics—the ATT, for example, is an arms control agreement negotiated in the UNGA and that grew out of the First Committee, and it has human rights squarely at its core. Moreover, respect for human rights is highlighted in the 2013 and 2015 reports of the GGEs on ICTs.

3. Finally, I want to highlight another dimension of threat which is probably less well-covered than some others but is relevant given that the OEWG grew out of the UNGA First Committee on Disarmament and International Security. And those are the vulnerabilities of existing weapons, and weapon systems, to hostile cyber operations.
   - For example, nuclear weapon systems, including those for planning, early warning, and communications, and delivery, as well as civilian nuclear energy production are vulnerable to in part because they are designed on outmoded and less protected technology, but also in the context of the widespread modernization programmes underway in all nuclear-armed states;
   - The rapid proliferation of armed drones, and potential development of autonomous weapon systems, present the possibility of network interference activities.
   - New modes of communication, information sharing, monetary exchange, etc. can also facilitate illicit arms sales or the sale or exchange of other materials that can be used in
weapons development. New technologies are also changing weapon production patterns, or marking and tracing practices for example of SALW.

- Perhaps the OEWG is not the correct forum to meaningfully take up this dimension in its future work but I highlight for member states to consider with respect to other fora that they participate in, such as the Arms Trade Treaty and UNPoA; the CCW; and the WMD-relevant treaties, and to see first how those instruments may need to be updated and adjusted to modern digital realities, but also to remind that these new risks and vulnerabilities are a powerful incentive to disarm.