UNODA United Nations Office for Disarmament Affairs

**UN Institute for Disarmament Research (UNIDIR)**
**Annual Cyber Stability Conference**

# "ICTs in the Context of International Peace and Security: Current Conditions and Future Approaches"

**Opening Remarks**

**by**

**Ms. Izumi Nakamitsu**
**High Representative for Disarmament Affairs**

11 October 2017
New York

Mr Jarmo Sareva, Director, UNIDIR

Distinguished Delegates,

Ladies and Gentlemen,

It is a pleasure to be here today at UNIDIR's Annual Cyber Stability Conference.
It is the first time that the Conference series is being held during the First Committee session in New York and it is very timely indeed.

We are at a critical juncture in the deliberations at the UN on how to deal with the use of information and communications technologies (or "ICTs") in the international security context.

The Chair of the most recent Group of Governmental Experts, Mr. Karsten Geier, is to be highly commended for his tireless efforts to find the path to consensus amongst the members of the Group, but in the end, the Group of Experts was not able to reach agreement on a final report.

The key question on all our minds here at First Committee this year is: what comes next?

Allow me to offer some thoughts on how we can move ahead together.

**First, we need to look backwards to move ahead.**

As we deliberate on what our next steps should be after the most recent Group of Governmental Experts, an important thing to keep in mind is that we already have three substantive reports from previous GGEs with important assessments and recommendations upon which to build our work.

I cannot emphasize enough that the validity of progress made in previous GGEs is without question. In particular, I would draw your attention to the resolution adopted by the General Assembly last year which "calls upon Member States to be guided in their use of information and communications technologies by the 2015 GGE report".

I strongly believe that there is a lot of valuable material to be found in these reports, including on the application of international law; on voluntary, non-binding norms of responsible State behaviour; and on confidence- and capacity-building measures in the use of ICTs.

One possible way forward which Member States may wish to consider is to call for a forum to take stock of the progress made in implementing these previous GGE reports.

My Office, with the support of the Government of Singapore, has also begun developing an online training course based on these GGE reports. We invite you to join with us both in the development of the modules and in participating in the training itself.

**Second, we need to create a more inclusive space.**

Since 2004, the UN General Assembly established five Groups of Governmental Experts to address ICTs in the context of international security. It has been unusual to hold consecutive GGEs without intermission.

Originally, these GGEs consisted of 15 Member States; they then expanded to include 20 States and most recently, 25. However, still less than 20% of the 193 UN Member State have been represented on these GGEs.

Cyber security is an issue that increasingly affects all countries and all, including the other 80% of UN Member States, should be given a voice in multilateral discussions.

Creating an inclusive space is not just about a broader platform, it is about finding a path forward that takes into account the input of all stakeholders.

The Groups of Experts have affirmed that while States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation of the private sector, academia and civil society organizations.

I believe a lot of work still needs to be done to create an inclusive space for the participation of these key actors in a sustained and meaningful manner.

At the High-Level event on "The roles and responsibilities of private actors in cyberspace" organized by the Permanent Mission of France last month, a key point raised was that Governments and the private sector in fact  need each other.

One of the arguments for this statement was particularly salient: Actors in the cybersphere have recently emerged that have resources to undertake offensive cyber operations so sophisticated that they cannot be defended by technology alone.

Policy and technology therefore need to go hand-in-hand, and this can only be done when Governments and the private sector cooperate effectively.

**Finally, we need to urgently return to first principles of agreement.**

The cyber threat is growing, but also increasing is the severity and destabilizing effects of cyber incidences. In November 2016, a country was taken offline due to a "botnet attack" that shut the system down by overwhelming it with traffic.

Earlier this year, Wannacry Ransomware reportedly affected around 200,000 systems in over 150 countries.

There also appears to be a trend in the manipulation of information online such as the planting of fake news which has affected State relations, and confidential information has been leaked in the context of national election processes.

These cyber incidents have a potentially destabilizing effect on countries, in regions and across the globe. It is this impact of the use of ICTs on international security that is particularly concerning.

The International Community needs to rally together now more than ever.

Returning to the GGE for a moment, I would like to highlight that despite divergent views, one important, unshakable point of agreement was that all Members of the Group have an enduring commitment to an open, secure, stable, accessible and peaceful ICT environment.

I personally take heart from this.

I urge all of us to begin again with this first principle of agreement and once more re-double our efforts to engage in serious dialogue, no matter how difficult, to build upon the good work already done, and move forward towards a peaceful cyberspace.

I wish you a fruitful conference ahead.
Thank you.