[check against delivery]

Security Council Arria Formula meeting

"Cyber Stability, Conflict Prevention and Capacity Building."

Statement by H.E. Timo S. Koster

Ambassador-at-Large of the Kingdom of the Netherlands

NEW YORK, 22 May 2020

Mr. President,

Thank you for bringing us together and initiating this debate in this time of crisis.

Mr President,
The Netherlands is strongly committed to promoting and upholding the international rules based order, as enshrined in the Dutch Constitution. Therefore, Digital Trust & Security is at the top of our list of priorities, in particular during these testing times.

It is very appropriate and timely that the Estonian Presidency has scheduled this session of the Security Council, the highest multilateral forum on the globe.

The mission we see in the Netherlands, which we would like this community to follow, is threefold

1. **We must consolidate the rules of the road in Cyber space**. International law applies in full, norms for state behavior have been agreed in 2015 and are being elaborated in two separate UN tracks as we speak. And with the development of new technologies we need to keep strengthening those rules. To make sure that use of ICT's and other technologies is safe and secure, and that the fundamental rights of each individual are respected.
   However, we see an unacceptable degree of non-compliance: critical infrastructure is being attacked including medical, even the public core of the internet. The Netherlands has advocated for declaring medical infrastructure off limits for cyber operations. This brings me to the second part of our mission:
2. **We must hold those who break the rules accountable**
   We must close the accountability gap ! Although we all agree on the norms and rules. Although again today around this table we seem to agree on what is and is not acceptable, malicious behavior is on the rise. The Netherlands is appalled by the abuse of the COVID crisis for cyber operations. So we need to work together on attribution, call out malign practices. Impose consequences. We need to build Alliances between public and private sector, with involvement of other stakeholders, to expose malicious behavior. And this includes exposing disinformation campaigns.
3. **We need to enable all nations to protect themselves.** Assist in building technical resilience, help drafting legislation that ensures internet safety and security, and at the same time respect for human rights. Make sure that everyone can reap the benefits of new technologies. And empower all states to take part in the global debate about our common digital future. Not out of charity, but in the interest of all of us. We encourage all to make good use of the Global Forum for Cyber Expertise, a Dutch initiative that has now matured into the world's strongest Capacity Building platform.

The fact that we're having this debate at the level of the Security Council is an important milestone. But let's make sure we involve other stakeholders as well. The private sector, civil society. These are the problems of our time. We need to seize this moment to speak up against abuse of the COVID-19 crisis to conduct cyber and disinfo operations. Similarly we need to seize the UN75 moment to highlight these challenges at HOSG level. And to carry this forward in a UN initiative on Digital Trust & Security for the year to come.

Thank you