PERMANENT MISSION OF THAILAND
TO THE UNITED NATIONS
136 EAST 39th STREET· NEW YORK, NY 10016
TEL (212) 754-2230 • FAX (212) 688-3029

Statement

Delivered by
H.E. Mr. Suriya Chindawongse
Ambassador Extraordinary and Plenipotentiary
and Permanent Representative of the Kingdom of Thailand
to the United Nations

At the First Substantive Session of
the Open-ended working group (OEWG) on security of and in the use of information and communications technologies 2021–2025

New York, 13-17 December 2021

Mr. Chair,

1. Thailand associates itself with the statements made by Indonesia on behalf of the Non-Aligned Movement and by Brunei Darussalam on behalf of the Association of Southeast Asian Nations or ASEAN.

2. At the outset, Thailand would like to join other delegations in congratulating His Excellency Ambassador Burhan Gafoor, Permanent Representative of Singapore, on your assumption of duty as the Chair of this working group. I am confident that, under your able leadership, our work will lead to fruitful and tangible outcomes. My delegation will give its full support to you, Mr. Chair, during the course of this session.

3. My delegation also wishes to thank His Excellency Ambassador Jürg Lauber of Switzerland for his able guidance that led to the success of the previous OEWG. The successful conclusion of the previous OEWG and of the 6th iteration of the GGE has laid down concrete steps for this new OEWG to build and expand upon.

4. Together with the successful adoption of the UNGA resolution "Developments in the field of information and telecommunications in the context of international security", tabled by the Russian Federation and the United States, and co-sponsored by Thailand, these important developments also reflect that, with mutual trust among Member States, we can achieve much more.

Mr. Chair,

5. The emerging and potential threats emanating from the misuse of ICTs, by both States and non-State actors, have increasingly become a serious threat to international peace and security, especially when reliance upon ICTs has expanded in our increasingly digitalized, interconnected and technologically-driven global economy. Malicious attacks on critical infrastructures (CI) and critical information infrastructures (CII) can potentially result in severe humanitarian impacts, amongst others, especially for developing countries. This issue thus requires cooperation on a global scale.

6. To foster such cooperation, we need to achieve a common understanding and seek further clarification on the pending issues. While States generally subscribe to the 11 voluntary, non-binding norms of responsible State behaviour and the international law applicable in cyberspace, we still lack a common understanding on *how* international law applies and *whether* the gaps exist, as well as how to operationalise these norms. There is a need to further develop guidance and recommendations on how to put these norms into practice.

7. As much as these issues should be discussed within the OEWG, States should also utilise regional mechanisms to further elaborate on these issues. As the first regional organisation to subscribe in-principle to these 11 voluntary, non-binding norms, ASEAN has embarked on a process of developing a matrix for ASEAN's plan of action on the implementation of norms of responsible States behaviour in cyberspace. Through this process, Thailand is working with other ASEAN Member States to translate these norms into practice. This is part and parcel of collective efforts to contribute to a safer and secure ASEAN Community.

8. These efforts, together with other mechanisms and capacity building efforts within the region, such as those carried out by the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok, serve as regional Confidence-Building Measures (CBMs). Thailand encourages similar practices in other regions, and we also support the establishment of cross-regional CBMs, as they would play an important role in encouraging and solidifying CBMs globally.

Mr. Chair,

9. Capacity-building can play a significant role in mitigating the impact of malicious cyber activities, and at the same time, empowering all States and other relevant actors to implement the relevant norms and international law. Capacity building also increases States' capacity to engage meaningfully in the discussion and thus helps the international community to better develop a common understanding on these issues. At this OEWG, States should further discuss how the UN can play a role in fostering international cooperation, and productive engagement of all States and relevant actors, on this issue.

10. In the implementation of capacity building efforts, Thailand urges all States to be guided by the principles contained in paragraph 56 of the Final Report of the previous OEWG – in particular, capacity building must be a sustainable-process, politically neutral, transparent, accountable, undertaken with full respect for the principle of State sovereignty, demand-driven and confidentiality of national policies and sensitive information must be ensured.

Mr. Chair,

11. Thailand welcomes further details on the specific proposal that has been made with regard to the establishment of a new mechanism aimed at promoting regular institutional dialogues among States. We look forward to engaging in a constructive dialogue with other States on this matter. We believe that in order for this new mechanism to be effective, it should be inclusive, pragmatic and action-oriented.

12. In conclusion, this 5-year OEWG presents an opportunity for all States to engage in the issues of cybersecurity, in particular to discuss *how* we can move forward and the *direction* in which we are moving towards. Thailand is fully committed to engage with all parties to enhance global cybersecurity in order to promote an open, secure, stable, sustainable, accessible, interoperable and peaceful ICT environment.

Thank you very much.
