Statement

Delivered by
Mr. Karin Kunjara Na Ayudhya,
First Secretary

On “Confidence-building Measures”
at the Informal Session of the Second 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, 30 March 2022
Mr. Chair,

1. Thailand would like to express our appreciation to the Chair for convening this timely meeting and reaffirm Thailand’s full cooperation to this crucial platform. Thailand associates itself with the statements made by Indonesia on behalf of the Non-Aligned Movement (NAM) and Cambodia on behalf of ASEAN and would like to make a few points on our national capacity.

2. At the first substantive session and throughout this session, several States have recognized the important role of regional organizations in forging trust, predictability, and stability in the use of ICTs by States. Thailand would like to echo that notion, and having carefully reflected on the Chair’s guiding questions, would like to focus this intervention by highlighting some examples and lessons on Confidence-building measures (CBMs) that we have been implementing at the regional level that could contribute to the consideration towards developing cross-regional and global CBMs.

3. First, a notable initiative that has been highlighted by several delegations throughout this meeting is the multi-year cyber-capacity building program focused on supporting the effective implementation of United Nations (UN) norms of responsible state behaviour in cyberspace throughout ASEAN. The initiative provided ASEAN Member States with a valuable opportunity to share and discuss good practices and policies. We invite all States to draw on the examples and lessons from this initiative, with hopes that it may inspire similar efforts in other regions. We thank the Governments of the United Kingdom and Australia, and the Australian Strategic Policy Institute for their generous support and partnership.

4. Second, drawing from Thailand’s experience, we believe that regional efforts in promoting CBMs should be centralized and guided by a comprehensive yet flexible joint plan. As is the case with ASEAN, the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) is key to advance the region’s efforts towards creating a secure, resilient, interoperable and rules-based cyberspace, which further reinforces ASEAN centrality. Moreover, in January 2022 ASEAN also has adopted Cybersecurity Cooperation Strategy 2021 - 2025, the latest joint plan that has been updated in response to new developments in ICTs. This allows ASEAN to continuously build on the progress while advancing the region’s cyber incident preparedness. At the global level, States may consider establishing similar mechanism or cybersecurity strategy to serve as global CBMs.

5. Third, regular consultation amongst all concerned parties is one way to form a good basis for CBMs, which would lead to sharing of information necessary to prevent cyber attacks. Therefore, constant updates and testing of Points of Contact
(PoCs) Directory are essential not only to responding to emergencies, but also to creating a pathway for trust and cooperation. Thailand and other ASEAN Regional Forum Member States have regularly updated our PoCs Directory on Security of and in the Use of ICTs. We thus support the establishment of the POCs Directory at the global scale, at the technical, policy and diplomatic levels, as well as their constant updates and testing, and regular dialogues among them. Thailand believes that this will serve as a good starting point for establishing CBMs at the global scale.

6. Fourth, drawing from ASEAN’s experience, Thailand believes that the OEWG can play a role in fostering international cooperation on CBMs, in particular, coordination between national Computer Emergency Response Teams (CERTs). We are of view that the establishment of a platform to enhance voluntary information exchange and cooperation amongst national CERTS is critical to strengthening trust amongst States, and subsequently result in strengthening our collective capacity to respond to the evolving cross-border challenges in cyberspace.

7. Finally, Thailand continues to benefit from several other noteworthy initiatives that seek to bring together cross-regional actors to exchange experience and information, including the Women and International Security in Cyberspace Fellowship organized by the United Nations Institute for Training and Research (UNITAR) and its partners and also the United Nations Institute for Disarmament Research’s (UNIDIR) Cyber Policy Portal. We support on-going efforts of various stakeholders that aim to foster opportunities and spaces for discussion.

I thank you, Mr. Chair.