Mr. Chair,

Thailand recognises that 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 norms of responsible State behaviour, as well as international law applicable in cyberspace. Capacity building also increases States’ capacity to engage meaningfully in the discussion on these issues and thus helps the international community to better develop common understanding on these issues.

This new OEWG framework is an opportunity for States to discuss the way forward on how the UN can play a role in fostering international cooperation on capacity building. In particular, coordination between national Computer Emergency Response Teams (CERTs) is one such area of interest. In this regard, capacity building will be key in facilitating the international community’s ability to prevent or mitigate the impact of malicious ICT activity through enhancement of the capacity of each State to prepare and respond, including the protection of critical infrastructures (CI) and critical information infrastructures (CII). In light of the COVID-19 pandemic, a particular emphasis should also be given to the protection of medical and public health critical infrastructure, as they are most at risk.

In the past few years, ASEAN has strengthened its capacity building cooperation under different frameworks, including through cooperation with dialogue partners. Thailand appreciates continued support from the Government of Japan for the funding of the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCC BC) in Bangkok, Thailand, with an aim of strengthening regional cybersecurity capacity-building in the region, particularly for the protection of critical information infrastructures.
Thailand urges all States to be guided by the principles contained in paragraph 56 of the Final Report of the previous OEWG in their implementation of ICT-related capacity building efforts – 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.

Thailand agrees with many delegations that a range of actors, including the private sector, academia and civil society have a role in contributing to building trust and confidence in the use of ICTs at national, regional and global levels. Developing digital literacy to actors as well as individuals helps increase States' and the international community's resilience against malicious cyber activities. Furthermore, such actors can and should facilitate resourcing of assistance as well as the establishment of cooperative mechanism or platform for capacity-building activities.

Thailand also recognizes the urgent need of capacity-building programmes in order to help bridge the digital divide. Therefore, we encourage States with the capacity in cybersecurity to provide transparent and demand-driven assistance to States with special needs.

I thank you Mr Chair.