Statement of the Dominican Republic, Estonia, Germany and Luxembourg regarding Capacity Building in the Latin America and Caribbean region.
16 December 2021

Thank you, Mr. Chair,

Let me express my sincere gratitude for your commitment to facilitating a practical discussion. In this spirit, I would now like to make a statement on behalf of the Dominican Republic, Estonia, Germany, and Luxembourg and present one concrete capacity-building initiative in the Latin America and Caribbean region.

As capacities to prevent and mitigate the impact of cyber-attacks vary highly among countries worldwide, we attach great importance to the topic under consideration this afternoon. To turn the recommendations of the successive GGE consensus reports and the latest OEWG consensus report into action and genuinely implement the framework for responsible state behaviour in cyberspace, capacity building is indispensable.

We are committed to having an open, free, secure and resilient cyberspace. Part of this commitment is finding opportunities to work together across national and regional borders to build capacity and strengthen cyber resilience of States so they can fully enjoy the benefits of the Internet and other digital technologies.

Recently, the Dominican Republic has started working with the European Union's CyberNet project with the support of the governments of Estonia, Germany and Luxembourg in an unprecedented effort to set up a Regional Cyber Training Centre that will support the Latin American and Caribbean Region to allow for a more targeted and systematic capacity building in the LAC region.

The Dominican Republic was chosen to host the first such centre in the region, given its close ties to North, Central and South America, and membership of regional

organizations like the OAS and CARIFORUM. This is further supported by the country's long history of international cooperation and assistance in matters pertaining to securing cyberspace, and agile organizational and procedural frameworks, which enable collaboration and trust between agencies, and a true whole-of-nation approach to cybersecurity and capacity development.

The Centre, which will have a physical base in the historic city centre of Santo Domingo, will be called the Latin America and Caribbean Cyber Competence Centre (or LAC4) and will become fully operational in early 2022. Its mission is to act as a regional knowledge hub and training centre to enhance cybercrime and cybersecurity education and training, improve interoperability and capabilities in cyberspace, including research and development as well as assist in national norm development. Specifically, it will serve as a hub for sharing the EU's collective expertise through specialized courses and workshops, building up local capacity based on Train-the-Trainer principles, facilitating practical collaboration between the region and the EU, and promoting the benefits of an open, free and inclusive cyberspace.

The principle target groups for the Centre's training activities will be national cybersecurity organizations and critical information infrastructure operators in both public and private sectors, as well as law enforcement specialized cybercrime units. The LAC4 would offer trainings both at strategic/policy and technical levels.

LAC4 will act as the key facilitator of the EU's cybersecurity projects in the region, providing a venue and technical training environment, and make available existing training modules and materials developed in the EU. The Centre's mandate will be complementary to regional efforts of strengthening cybersecurity and combatting cybercrime by the Organization of American States (OAS), Caribbean Community and Common Market (CARICOM) and other international organizations.

The Centre will be leading the development of a cybersecurity research roadmap at regional level, setting priorities for the next 5 to 10 years. As such, the LAC4 will serve as a nexus for coordinating research efforts for the benefit of the entire region.

Additionally, LAC4 shall develop into a multi-nationally sponsored entity engaging with national and international, governmental, academic and private stakeholders to explore the possibilities of cooperation. This includes seeking partnerships with the private sector and offering customer-funded slots for SMEs for to contribute to the LAC4's financial sustainability scheme.

The Centre is an example of what can happen if you put together ambition, experience and a joint commitment to the framework for responsible behaviour in cyberspace. We would be happy to provide further information on the initiative as well as discuss opportunities to become a LAC4 Participant Nations or Contributing Partner.

Thank you Mr. Chair.

Key elements to highlight

The Centre should foster cybersecurity skills development and lead to the overall increase of trained experts in the LAC region.

In this context, countries in the region will be better prepared to counter cyber threats, have improved regional cooperation in cybersecurity and countering cybercrime, and have stronger collaborative relationships with the EU for information sharing and incident response.