This project is funded by the European Union

CYBER RESILIENCE FOR DEVELOPMENT (CYBER 4D)

PROJECT PURPOSE:

This EU funded project will aim at increasing the security and resilience of critical information infrastructure and networks supporting the critical services of third countries (Africa and Asia) while ensuring compliance with human rights and the rule of law, through the adoption and implementation of a comprehensive set of policy, organisational, and technical measures.

PROJECT COMPONENTS / EXPECTED RESULTS:

This action, financed by the Instrument contributing to Stability and Peace (IcSP), contributes to the **overall objective** to "allow the citizens of developing countries enjoy the digital dividends of an open, free, secure and resilient cyberspace" in line with the IcSP Strategy (2014-2020) and (Multiannual Indicative Programme) MIP (2014-2017) that foresees the promotion of cyber resilience through "raising awareness on cyber threats; developing national cyber security strategies; providing for information assurance and resilience; setting up, training and equipping Computer Emergency Response Teams, building early warning, information sharing and analysis capabilities in priority regions" as the main aim of the "Protecting Critical Infrastructure" priority.

The **specific objective** of the proposed action is to increase the cyber resilience of third countries while promoting an inclusive multi-stakeholder and rights-based approach and ensuring compliance with the rule of law and good governance principles. This will be pursued by supporting the adoption and implementation of a comprehensive set of policy, organisational, and technical measures.

In terms of **tangible results**, this should lead to the following:

- countries have increased political will to act on cybersecurity
- countries supported to devise a new cybersecurity strategy or have started implementing an existing strategy
- countries have established democratic and inclusive multi-stakeholder governance structures for developing and implementing a cybersecurity strategy
- countries/regions have stronger, more effective collaborative relationships on cybersecurity and incident handling.
- countries/regions have improved CSIRT capability and more effective collaborative relationships with the EU for information sharing and incident response.
- countries have improved coordination between authorities in charge of cybersecurity and cybercrime.
- countries have included measures to protect human rights, rule of law and vulnerable individuals within their cybersecurity strategies/policies/laws.
- EU trading partners have improved cybersecurity and better conditions for growth.
- The EU is helped to counter cyber threats and foster the cyber resilience of the EU and its partners.

In order to meet the objectives mentioned above, the action is designed to deliver three **outputs** (results), described below that are mutually reinforcing, building on a national, regional and

transregional approach, promoting EU best practice and ensuring compliance with the principles of inclusive multi-stakeholder and rights-based approach, the rule of law and good governance.

Output 1: Strengthened Cybersecurity Policy, Strategical, and Coordination Frameworks

Increased awareness of decision-makers on cyber security issues and facilitation of adoption and implementation of consistent, holistic and actionable national cybersecurity strategies in priority countries. The engagement in this field shall be based on a multi-stakeholder approach that promotes the establishment of appropriate coordination frameworks and structures amongst public sector entities themselves and also with the private sector, both at policy and operational levels, while ensuring compliance with the rule of law and good governance principles.

Output 2: Increased Cybersecurity Incidence Response Capabilities

Increased local operational capacities to adequately prevent, respond to and address cyber security incidents through strengthened Computer Security Incident Response Teams and improved formal and informal cooperation in the national cyber ecosystem of priority countries.

Output 3: Fostered Networks of Cyber Expertise and Cooperation

Intensified awareness and promotion of cybersecurity good practices globally on the basis of EU expertise and increased trust and enhanced regional, trans-regional and international cooperation on cyber security issues through the promotion of formal and informal networks for sharing of best practices and incident information.

IMPLEMENTING PARTNERS:

- Foreign and Commonwealth Office (FCO), UK
- Dutch Ministry of Foreign Affairs (MFA), NL
- Estonian Information System Authority (RIA), EE

PROJECT LOCATION:

In the preparatory phase of the action an analysis was undertaken to identify a number of potential hub and priority countries. The following countries have been agreed as priorities.

- West Africa: Senegal, Ghana
- Central Africa: Rwanda
- East Africa: Mauritius
- Southern Africa: Botswana
- South Asia: Sri Lanka

PROJECT DURATION: 42 Months