Presentation on EU Cyber Capacity Building efforts

OEWG 27 July 2022, New York
External cyber capacity building is a **strategic building block of EU's cyber diplomacy** as outlined in the EU's Cybersecurity Strategy and other policy documents such as EU's Digital4Development Strategy and the Global Gateway.

The EU's **aim** is to support partners in addressing their key cyber-related needs, including strengthening societal resilience, building trust in the digital environment, protecting human rights and freedoms, or participating in international processes.

**Focus** on (1) strengthening national capabilities (e.g. organisational structures, processes and networks), (2) strengthening collective capabilities (through whole-of-society approach) and (3) facilitating international cooperation and partnerships (e.g. through institutional, legislative and policy frameworks)

EU capacity building efforts are **needs driven** and implemented in line with its values, interests and principles.
EU external cyber capacity building

- The EU's financial commitment has increased over years from EUR 10 million during the 2007-2013 budget to EUR 95 million during the 2014-2020 budget. Cyber mainstreamed in the 2021-2027 budget for capacity building and part of geographic, thematic and rapid response pillar (total of EUR 79.5 billion).

- The EU is currently funding over 30 projects addressing cybersecurity (e.g. Cyber4D), cybercrime (e.g. Glacy+, iProceeds and OCWAR-C) and cyber diplomacy (e.g. EU Cyber Direct, Security in/with Asia)

- The EU has been systematically linking its capacity building with development and international cooperation funds in five pillars: national strategic framework, criminal justice in cyberspace, cyber crisis prevention and management, cyber hygiene and awareness, cyber diplomacy.
Developments in external cyber capacity building

1. **More financial resources available and more actors involved**
   Enhanced need for coordination within the EU and with international partners, notably through the GFCE and the proposed Cyber Programme of Action.

2. **Scope of EU cyber capacity building is expanding**
   EU cyber capacity building efforts include cybersecurity, cybercrime and cyber diplomacy.

3. **Complexity and interlinkages are growing**
   Need to mainstream cyber into other capacity building efforts, including on digital development.

4. **Cyber capacity building needs are increasing due to rising cyber threats**
   Requires to step up both the quantity as well as quality of EU external capacity building efforts.
EU ambition: collaborative transformation

1. **Investment growth driven by common goal** of ensuring all states, citizens and businesses can benefit from safe, resilience and accessible technologies.

2. **Idea of common principles** of cyber capacity building gain traction.

3. **More actors involved see the benefits in coordination** of cyber capacity building efforts.
EU developments

2018 – 2019

• EU External Cyber Capacity Building Guidelines that define scope, principles and the EU approach.
  • EU Operational Guidance for project implementers.
  • Establishment of EU CyberNet: building the EU's capacity to deliver cyber capacity building and enhances coordination among projects, including through the Latin America and Caribbean Cyber Competence Centre LAC4.
EU developments

2020 – 2021

- Establishment of an EU Cyber Capacity Building Board to facilitate EU coordination, as well as with other partners and stakeholders.
  - Enhance cooperation with the multi-stakeholder community in view of coordination as well as utilising research efforts to support an evidence based approach.
  - Continuous mapping of EU and EU Member States' cyber-related external capacity building efforts, including as input for the Global Forum on Cyber Expertise (GFCE) Cybil Portal.
• In the context of the proposal on a UN Programme of Action, development of a Multilateralism and Digitalisation (M&D) programme to build capacities on the application of international law and norms of responsible state behaviour.

• **Development of an EU cyber mainstreaming toolbox – mainstreaming cyber into all relevant EU capacity building programmes.**

• **Analyse lessons learned to support the update of the 2018 Operational Guidelines**