The EU's efforts on external cybersecurity capacity building

Promoting a 'whole-of-government' approach

European External Action Service
Heli Tiirmaa-Klaar
Head of Cyber Policy Coordination

EU principles and values on cyberspace issues

Strategic priorities:

1. Achieving cyber resilience
2. Drastically reducing cybercrime
3. Developing cyber defence related to CSDP
4. Developing industrial and technological resources for cybersecurity
5. Establishing an EU international cyberspace policy

Roles and responsibilities between actors in EU

Cyber Resilience

A technical issue?

A security issue?

A legal issue?

A financial issue?

A defence issue?

A development issue?

NEXUS: a multi-layer governance issue

Setting the Scene

- **Cybersecurity:** a way to empower individuals, communities and governments to achieve their developmental goals by reducing digital security risks stemming from access and use of ICT.

- **Risks:** not only those posed by either state or non-state actors to another state and its citizens (i.e. loss of data, attacks on government websites), but also those resulting from a state's negligence or premeditated actions against its own citizens.

- **Security:** not only as a goal per se but also an enabler of political, social and economic transformation that may not always be identical to security objectives as defined by a state.

Setting the Scope

- **Need for conceptual clarity:**
  Cybercrime and cybersecurity
- **Need for stakeholders' mapping clarity:**
  Cybercrime: criminal justice actors + PPPs
  Cybersecurity: whole-of-government approach + PPPs+international cooperation
- **Approach:**
  Integrating EU internal experience, **existing best practice** and **common standards** with **lessons learnt** from development cooperation

Cybercrime - Focal engagement areas:

1. Facilitating the development or reform of **appropriate legal frameworks** (substantive and procedural) in compliance with international standards (Budapest Convention on Cybercrime), due process, human rights and in a manner that fosters greater international cooperation.

2. **Enhancing the capacities of criminal justice authorities**, such as law enforcement, prosecutors and judges, in order to enable them to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence.

Examples of EU-funded actions in Fighting Cybercrime

1. ‘Global Action on Cybercrime’ (GLACY)
Council of Europe (3.35MEUR, Nov 2013 – Oct 2016)
Priority countries: Mauritius, Morocco, Philippines, Senegal, Sri Lanka, South Africa, Tonga
Project Partners: EC3/Europol, France, Romania

2. ‘Global Action on Cybercrime extended’ (GLACY+)
Council of Europe, Interpol (10MEUR, Mar 2016 – Feb 2020)
Priority/Hub countries: Dominican Rep., Ghana, Mauritius, Morocco, Philippines, Senegal, Sri Lanka
Project Partners: EC3/Europol, Estonia, France, Romania, UK/NCA, US/DoJ

Objective: To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

Cybersecurity-
Focal engagement areas:

1. Supporting the development of **organisational, technical and cooperation mechanisms** that increase cyber resilience and preparedness:
Facilitating the development of **national cybersecurity strategies**.

2. Setting up **functional incident response structures / national Computer Emergency Response Teams**.

3. Promoting **effective** inter-institutional, inter-agency and international **cooperation** as well as public-private exchanges.

Examples of EU-funded actions in Promoting Cyber Resilience

1. Enhancing Cybersecurity (ENCYSEC)

Expertise France & Civi.Pol Conseil (1.5MEUR, 2014 – 2016, pilot)
Priority countries: Kosovo* (*UNSCR 1244/1999,ICJ 2010), Former Yugoslav Republic of Macedonia, Moldova
Close collaboration with Romanian and Czech CERTs

2. Cyber Resilience for Development

NI-CO with UK/FCO, NL/MFA&NCSC, EE/RIA, DE/GiZ
Geographical focus: Africa, Asia (11 MEUR, 2017-2020) to commence in mid 2017
Objective: Support the adoption and implementation of a comprehensive set of policy, organisational, and technical measures that will increase their cybersecurity preparedness, following a multi-stakeholder and human rights compliant approach.

Mainstreaming Cybersecurity

Security an afterthought?

An ever vulnerable digital domain

Digitalisation without embedded security:

•vulnerable, non-resilient systems

•unsustainable investments

• security added by patchwork

Challenge

Digital ecosystem
that is secure by design

vs

patching leaking buckets
while the tap is open