Towards operational guidance for the EU's cyber capacity building abroad

Consultation on the draft operational guidance

This project is funded by the European Union

16 May 2018, Martin's Hotel, Amber+Bronze Meeting Room
Boulevard Charlemagne 80, Brussels

Concept

The expanding use of Information and Communications Technology over the past 20 years and its contribution to the evolution – or even complete revolution – of various policy areas has resulted in the emergence of a broad policy community relying on these technologies. However, efforts at improving access to ICT and growing levels of internet penetration have so far underestimated the risks and challenges associated with this process. Consequently, capacity building has become a key approach which endeavours to ensure a minimum level of cybersecurity across the globe.

In broad terms, capacity building in the cyber domain is aimed at **enabling and strengthening functioning and accountable institutions to respond effectively to cybercrime and to enhance the countries' cyber resilience**. This is an integral component of international cooperation and as such can foster international solidarity with the EU's vision to secure a free, open, peaceful, secure, interoperable cyberspace for everyone while ensuring compliance with human rights and the rule of law. The question about **how to structure the capacity building efforts, what methods to use and how to measure their efficiency** is a central one in this process.

Since the adoption of its **2013 Cybersecurity Strategy**, the EU has been leading on international cyber capacity building and systematically linking these efforts with its development cooperation funds. Such actions are based on promoting a rights-based and whole-of-government approach that integrates lessons learnt from EU's internal experience, as well as from the development effectiveness agenda. Moreover, in 2017 there has been a clear recognition at EU level that cybersecurity should be considered as a transversal issue in development cooperation that can contribute to the progressive realisation of **the 2030 Agenda for Sustainable Development**, as stipulated in the EU's Digital4Development policy framework. The significance of efforts to build national resilience in third countries as means to increase the level of cybersecurity globally, with positive consequences for the EU, was also recognised in the **Joint Communication on 'Resilience, deterrence and defence: building strong cybersecurity for the EU'** presented as part of the latest EU cybersecurity package in September 2017.

In light of this, a concerted effort is deemed necessary to **consolidate the lessons learnt from the EU's experience to date** – particularly in bridging the development and technical communities – as well as to combine the several dimensions of cyber policy with development cooperation principles into and into a systematic methodology that will serve as **operational guidance when designing and implementing EU's external cyber capacity building actions**. Due to the highly sensitive aspects of cybersecurity and potential flow-on risks running contrary to key EU values and policies (e.g. a rights-based approach, freedom of expression online/offline, multi-stakeholder internet model, the applicability of international law in cyberspace), vigilance is necessary to ensure coherence between EU policy and programmes.

Objective

On 16 May 2018, the **European Commission's Directorate General for International Cooperation** (DEVCO) in partnership with the **EU Institute for Security Studies** (EUISS) will host a consultation workshop in Brussels to present to a range of relevant stakeholders a draft study on the "Operational Guidelines for the EU's Cyber Capacity Building in third countries" which shall serve as a toolkit for the preparation and implementation of relevant EU-financed actions.

The Guidance is intended to provide a comprehensive practical framework on the EU's external actions in the fight against cybercrime and the promotion of cybersecurity and cyber resilience. The document aims to:

- provide a consolidated presentation of key aspects of cyber policy;
- assist in the design of appropriate, context-specific project interventions for cyber capacity building in third countries, drawing from development best practices and lessons learned; and
- propose metrics and indicators for measuring the results of cyber programming.

The draft study has been prepared by the EU Institute for Security Studies with expert input from its Cyber Capacity Building Task Force comprising academics, think tank experts and EU government officials. The document builds on a series of consultations held between October 2017 and April 2018 with relevant stakeholders, mainly EU services, EU Member States representatives, cyber and development experts, international organisations and civil society.

This consultation will bring together a mix of policy actors that have been working in the fields of cyber policy and cyber diplomacy, together with practitioners involved in the definition and implementation of cyber capacity building actions and experts in evaluating capacity development results with the objective to:

- present a draft version of the Operational Guidance study;
- collect inputs and comments that will feed into the final draft of the study; and
- exchange knowledge over the topic of external cyber capacity building in general.

The draft study will be shared with the participants before the meeting who will be invited to submit written comments, before or shortly after the consultation, to allow for incorporation of pertinent suggetions before the finalisation of the document which shall be made public in June 2018.

Registration

To confirm your attendance, please fill in a short registration form via this link by 15 May 2018.

Should you have any question, please contact Nayia Barmpaliou (panagiota-nayia.barmpaliou@ec.europa.eu) and/or Patryk Pawlak (patryk.pawlak@iss.europa.eu).

Agenda

12:30-13:30

Registration and lunch

13:30-13:45

Welcome remarks

Olivier LUYCKX
Head of Unit 'Security, Nuclear Safety', Directorate General for International Cooperation and Development, European Commission

Gustav LINDSTROM
Director, EU Institute for Security Studies

13:45-14:45

Session I: Introduction to the Operational Guidance

Overview of the scope and challenges, concepts, policy dilemmas, and presentation of the overall approach

Moderator

Patryk PAWLAK
Brussels Executive Officer / Project Coordinator, EU Institute for Security Studies

Presenters

Andrea CALDERARO
Director, Centre for Internet and Global Politics, Cardiff University

Maria Grazia PORCEDDA
Research Fellow, University of Leeds

Thorsten WETZLING
Privacy Project Director, Stiftung Neue Verantwortung

14:45-15:00

Coffee break

15:00-16:15

Session II: A framework for the EU's external cyber capacity building

Presentation of the conceptual framework and methodology for the EU's approach to external cyber capacity building

Moderator

Nayia BARMPALIOU
Policy Officer / Programme Manager for Organised Crime and Cyber, Directorate General for International Cooperation and Development, European Commission

Presenter

Patryk PAWLAK
Brussels Executive Officer / Project Coordinator, EU Institute for Security Studies

16:15-16:30

Closing remarks

Heli TIIRMAA-KLAAR
Head of Cyber Policy Coordination, European External Action Service

Nayia BARMPALIOU
Policy Officer / Programme Manager for Organised Crime and Cyber, Directorate General for International Cooperation and Development, European Commission