AUC set to hold First African Forum on Cybercrime

African Union Headquarters | Addis Ababa, Ethiopia
16-18 October 2018

[Addis Ababa, 16 October 2018] *The African Union Commission, together with a number of partnering organisations, holds the first continent-wide African Forum on Cybercrime from 16 to 18 October 2018 in Addis Ababa, Ethiopia bringing together more than 250 delegates from across the continent.*

In an increasingly digitalised world, more and more crimes either take place in cyberspace or may involve evidence in electronic form. Cybercrime is a borderless and global phenomenon and requires that governments be ready to cooperate and protect their citizens' rights also in cyberspace.

The African continent shows one of the fastest growth rates in Internet users worldwide, with digital connectivity that has almost tripled in the past five years. Cyberspace has become an essential tool for communication, innovation, social development and economic progress across the board. On the other hand, both government institutions and companies in Africa have been facing an increasing number of cyber-attacks, in line with global trends.

"It is our task and collective responsibility to build a Safe, Secure, Trustworthy and Inclusive Cyberspace for the benefit of all African people and States" said the *Commissioner for Infrastructure and Energy*, H.E. Dr. Amani Abou-Zeid, speaking ahead of the Forum.

On his part, the Deputy Head of the *European Union Delegation to the African Union*, Mrs. Anna Burylo, said "Everywhere in the world today societies are increasingly dependent on electronic networks and information systems. While digitalisation offers tremendous development opportunities, it also comes with serious potential vulnerabilities. The evolution of information communication technology has seen in parallel the development of criminal activity that threatens citizens, businesses, governments and critical infrastructures alike: cybercrime. It is a borderless problem… and it needs to be tackled jointly. The European Union therefore strongly believes that we need to work together at all levels to address it and we invest in international cyber cooperation in parallel with our internal efforts for cybersecurity".

"Large-scale theft of personal data, bullying, harassment and other forms of cyber violence, or sexual violence against children online are attacks against human rights. Attacks against computers and disinformation used in elections are attacks against political stability. Daily attacks against critical infrastructures affect national security and economic prosperity. The need for international organisations to join forces and enable governments and societies to meet the challenge of cybercrime has been recognised for many years. This Forum is a crucial step in this direction", further emphasized Alexander Seger who is the Executive Secretary of the *Committee of the Budapest Convention on Cybercrime at the Council of Europe*.

The first **African Forum on Cybercrime is a response to this need**: it is a joint effort to bring together regional and international organizations and national governments to discuss about national policies and legislation, international cooperation and how to strengthen capacities of criminal justice authorities.

Several mechanisms and instruments exist to assist African governments in developing their cybercrime laws and mechanisms to facilitate cooperation with other countries. The African Union's [Convention on Cyber Security and Personal Data Protection](#), also known as the Malabo Convention, and the Council of Europe's [Budapest Convention on Cybercrime](#) are the most relevant regional and international legal instruments in matters related to cybercrime, electronic evidence and personal data protection, and many national laws across Africa and the world are drafted based on the standards set up in these treaties.

The *Council of Europe* and the *European Union* also assist countries worldwide through a range of joint projects to develop cyber capacities and to enhance cooperation internationally within the framework of the Budapest Convention.

The **Forum** brings together more than 250 delegates from policy makers, legislative bodies and criminal justice authorities of 50 African countries, regional organizations, national governments, international institutions and private sector, focusing on three main streams:

(1) **Cybercrime policies and legislation**, international standards and good practices;
(2) **International cooperation** against cybercrime;
(3) **Capacity building** to empower criminal justice authorities to deal with cybercrime cases.

International experts, from Africa and from the rest of the world, will be leading discussions on current threats and issues, best practices, and the way forward.

The Forum is organized by the African Union Commission with the support of the Council of Europe, the European Union, INTERPOL, UNODC, the Commonwealth Secretariat, the U.S. State Department and the UK Home Office.

INTERPOL's connectivity among its 192 member countries provides the law enforcement community vast potential to reveal the global picture of the cyber criminals. Through this Forum, INTERPOL aims to make Africa's voice heard and extended to the other regions, and in turn energise the law enforcement community around the globe.

UNODC's Global Programme on Cybercrime is aimed at increasing efficiency in the investigation and prosecution of cybercrime, especially in relation to online child sexual exploitation is also addressed to African countries. Furthermore, the Regional Programme for Eastern Africa (2016-2021) contextualises UNODC capacity building initiatives in line with strategic regional and national priorities, as identified and agreed upon by member states.

The Commonwealth Secretariat is working with member countries in Africa to develop appropriate response and build resilience to the threats of cybercrime. In this regard, the Secretariat, working under the auspices of the Commonwealth Cybercrime Initiative and the Commonwealth Cyber Declaration will conduct a cyber-resilience review in The Gambia, Kenya and Namibia with a view to strengthening their legislative and institutional response to cybercrime.

In April, Commonwealth Heads of Government adopted a Commonwealth Cyber Declaration that sets out a common commitment to a free, open, inclusive and secure cyberspace, respecting human rights and freedom of expression.

The **African Forum on Cybercrime** takes place at the Headquarters of the **African Union Commission** (Roosevelt Street - Old Airport Area, W21K19, Addis Ababa, Ethiopia) from 16 to 18 October 2018.

Media representatives are invited to attend the press conference on Thursday, 18 October from 15h30 to 16h00.

Contacts:

At the African Union Commission:

Moctar YEDALY
Head Information Society Division
African Union Commission
Addis Ababa, ETHIOPIA
Tel:
Email: YedalyM@africa-union.org

At the Council of Europe:

Matteo LUCCHETTI
Project Manager
Cybercrime Programme Office (C-PROC)
Council of Europe (C-PROC), ROMANIA
Tel: +40 (745) 610 046
Email: Matteo.LUCCHETTI@coe.int

ABOUT THE ORGANISING PARTNERS

The European Union and the Council of Europe

The Council of Europe helps to protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime and its Protocol on Xenophobia and Racism, the Cybercrime Convention Committee (T-CY) and the technical cooperation programmes on cybercrime.

The GLACY+ project on Global Action on Cybercrime Extended is a Joint project of the European Union (Instrument Contributing to Peace and Stability) and the Council of Europe. GLACY+ supports twelve priority countries in Africa, Asia-Pacific and Latin America and the Caribbean region to strengthen their capacities to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area. These countries may serve as hubs to share their experience within their respective regions.

INTERPOL

Cybercriminal activity is moving faster at a global scale which has never been seen before. While it remains a challenge for the law enforcement community to move faster than the cyber criminals, INTERPOL's connectivity internationally with 192 member countries provides the law enforcement community vast potential to reveal the global picture of the cyber criminals and dismantle their networks. Collaboration among 192 member countries can and should be rooted in the harmonization among them to optimise outcomes.

Through this Forum, INTERPOL aims to make Africa's voice heard and extended to the other regions, and in turn energise the law enforcement community around the globe.

UNODC

As guardian of the United Nations Convention against Transnational Organised Crime and its supplementary Protocols, UNODC is committed to promoting compliance with relevant international obligations as well as to capacity building for criminal justice entities, including law enforcement agencies in Africa, in compliance with these obligations.

As such, UNODC is mandated to assist member states to prevent, and prosecute transnational organised crime and other serious crimes, including cybercrime, through capacity building and technical assistance. UNODC does so through its Global Programme on Cybercrime and respective Regional Programmes for Africa, but also through cooperation and partnership with other international organisations as well as NGOs and the private sector as a vital part of UNODC's capacity building strategy. The key objectives of the Global Programme are to increase efficiency in the investigation and prosecution of cybercrime, especially in relation to online child sexual exploitation and abuse; strengthened inter-governmental cooperation and also creating stronger links between law enforcement and private sector companies. In turn, the respective UNODC Regional Programmes, including the Regional Programme for Eastern Africa (2016-2021), contextualise UNODC capacity building initiatives in line with strategic regional and national priorities, as identified and agreed upon by member states.

The Commonwealth Secretariat

In April, Commonwealth Heads of Government adopted a Commonwealth Cyber Declaration that sets out a common commitment to a free, open, inclusive and secure cyberspace, respecting human rights and freedom of expression.

The Commonwealth Secretariat with support from the Foreign and Commonwealth Office's Commonwealth Cybersecurity Programme is working with member countries in Africa to develop appropriate response and build resilience to the threats of cybercrime. In this regard, the Secretariat, working under the auspices of the Commonwealth Cybercrime Initiative and the Commonwealth Cyber Declaration will conduct a cyber-resilience review in The Gambia, Kenya and Namibia with a view to strengthening their legislative and institutional response to cybercrime. The Secretariat will also assist Commonwealth countries in Africa to strengthen international investigation of cybercrime cases by implementing a network of cybercrime points of contact in all Commonwealth member countries. The network will improve information sharing of electronic evidence sharing for cross border investigations.