

SECOND AFRICAN FORUM ON CYBERCRIME

**Cybercrime policies and Legislation,
investigation,
International Cooperation**

Conference Programme

Online, 28 – 29 June 2021

Organized and funded by:



Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Outline

Background and Justification

As the world evolves towards a new “normal”, the use of and reliance on information technology has become more and more pervasive in society. Targeting and illegally exploiting computer systems and malicious software have also become increasingly common. The COVID-19 global pandemic has spurred an unprecedented increase in cyber-based illegal activities.¹ Offences involving computers have grown rapidly both in number and in sophistication, and even more alarmingly since the beginning of the pandemic.

In line with this global trend, the African continent – the fastest growing region of the world for Internet penetration and for use of mobile-based financial services, has become an increasingly attractive area for cybercriminals. Developing effective countermeasures has proven to be challenging in the global context, as well as aligning legislation, strategies and policies in a consistent and harmonized manner. As shown in recent reports^{2,3,4}, heterogeneous legal frameworks, lack of national strategies, and information infrastructures that are still scarcely secured in a number of countries, has made the African region a vulnerable target for cyber-criminal activities. A direct impact is evidenced not only on citizens, but also – and most worryingly – on the social stability of the States.

Many countries in Africa have made it a high-level priority to focus on developing cybercrime laws and policies capable to efficiently criminalize such illegal acts and allow effective international cooperation between criminal justice authorities, in line with international standards. In such an effort, a major point of attention has been the need to uphold fundamental rights of individuals – whether suspects or victims, while ensuring necessity and proportionality in the application of criminal justice. In such a context, law enforcement officers, prosecutors, magistrates and judges are called to fulfil their respective roles in increasingly complex environments, which require up to date skills and adequate tools, both technical and legal.

Support to this endeavor has been provided in the recent years by an increasing number of international and regional organisations. The much needed cooperation is imperative. It has become essential to join forces with each other and with national authorities, develop synergies in a consistent manner and deliver effective capacity building initiatives.

The benefits of such a cooperative approach was reconfirmed on the occasion of the First African Forum on Cybercrime, organized in October 2018 by the African Union Commission in Addis Ababa, and substantially supported by the Council of Europe, INTERPOL, the European Union, UNODC, the Commonwealth Secretariat, the UK FCO, the U.S. Department of State and the U.S. Department of Justice.

The more than 50 African countries that took part in that event agreed on the need to encourage further cooperation and exchange of experience within African continent, thus establishing the African Forum on Cybercrime as a recurrent initiative, to be organised every two years. The Second African Forum on Cybercrime will build on the conclusions drawn in 2018 and will focus on promoting mutual dialogue among national institutions and international organizations. The Forum will be an opportunity to assess the progress achieved by the many

¹ Microsoft. ‘Exploiting a Crisis: How Cybercriminals Behaved during the Outbreak.’ <https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak>

² Nir Kshetri (2019) “Cybercrime and Cybersecurity in Africa” *Journal of Global Information Technology Management*, 22:2, 77-81

³ Africa Portal, 5 February 2020. [Cybercrime and data privacy: how Africa can up its game](#)

⁴ CGTN, Unveiling the Cost of Cybercrime in Africa, 27 October 2020. [Unveiling the cost of cybercrime in Africa](#)

African countries that initiated legislative and policy reforms in the area of cybercrime and facilitate the exchange of knowledge and practical experience from successful operations conducted in these years.

The Forum is organized by the African Union Commission, the European Union and the Council of Europe (GLACY+ and Octopus projects) in partnership with other partners and comes as a reassurance of the joint commitment to work together towards finding new modalities of strengthening international cooperation against all forms of cybercrime.

The Forum will be organized as an online event of two days, respectively focusing on:

- ▶ **Cybercrime policies and legislative updates in Africa**
- ▶ **International cooperation on cybercrime and electronic evidence**

Hubs

In parallel to the online participation in the event, interested countries and/ or organizations can organize "hubs" to broadcast all or part of the Forum sessions.

If allowed by the COVID-19 countermeasures in place, Forum hubs are expected to host physical gatherings of local counterparts as side events of the main online conference, livestreaming a number of its sessions.

Such side events could focus on topics connected to the main streams of the Forum and could be organized in the form of hybrid events, with variable duration and format, to be decided under the leadership of local organizers.

Forum hubs are encouraged to ensure broad national media reach.

Organizational support, including provisioning of the venue and other services that may be needed, can be covered by the Council of Europe and other supporting institutions or partnering initiatives.

Council of Europe will host a side hub dedicated to Cybercrime investigations in practice. It is expected to gather speakers from several international organizations and African countries and to facilitate sharing experiences among participants about new cybercrime trends and ways to tackle cybercrime at a regional and international level.

Interpol will host regional hubs through their four offices in Harare (Zimbabwe), Nairobi (Kenya), Yaounde (Cameroon) and Abidjan (Côte d'Ivoire).

Supporting Organisations / Institutions

The African Forum on Cybercrime is organized by the **African Union Commission** and supported by a number of partnering organisations:

- ▶ **The Council of Europe;**
- ▶ **The European Union;**
- ▶ **INTERPOL;**
- ▶ **U. S. Department of Justice;**
- ▶ **U.S. Department of State**
- ▶ **[Others TBC]**

A number of regional organisations will also be invited to participate in the Forum, including: [TBC - the Economic Community of Central African States (**ECCAS**); the Common Market for Eastern and Southern Africa (**COMESA**); the Intergovernmental Authority for Development (**IGAD**); the Southern African Development Community (**SADC**); the New Partnership For

Africa's Development (**NEPAD**); the Economic Community Of West African States (**ECOWAS**); the East African Economic Commission (**EAC**); the Union Maghreb Arab (**UMA**); the African Union Mechanism for Police Cooperation (**AFRIPOL**) and the African Centre for the Study & Research on Terrorism (**ACSRT**)]

Expected results

The 2nd edition of the African Forum is expected to build on the results achieved following the 1st African Forum by contributing to:

- Sharing experiences among participants about new cybercrime trends and ways to tackle cybercrime at a regional and international level;
- Achieving a common understanding of cybercrime laws in the African countries, identifying potential gaps and launching a discussion on best practices;
- Facilitating international cooperation between criminal justice authorities of African countries, building cyber-capacity and promoting the adoption of international standards in the field.

Participation of national delegations and inputs on the discussion subjects is expected and encouraged. It is anticipated that the conference would produce recommendations and conclusions for further follow-up with individual countries.

Participants

Countries will be invited to nominate 10 participants each, particularly, including policy makers and legislators, representatives from the criminal justice sector (prosecutors, judges, law enforcement), delegates from ministries responsible for implementation of cybercrime and cyber security policies, and other national stakeholders with an active role in the cybercrime domain.

Online platform

The workshops will be held remotely via a video-conferencing platform. The format of the workshop is a response to the current COVID-19 pandemic, which prohibits international travel and the physical participation to events in large groups without endangering public health.

Interpretation

Simultaneous interpretation EN/FR/PT/AR will be provided.

Communication and visibility

The Forum will be given adequate visibility through a dedicated communication plan funded by the Council of Europe, which will include the creation of specific areas on the web for participants to accede to contents, live streaming and recorded sessions.

Draft agenda

The Forum will consist of 2 online sessions of 3h30 each, organized in a period of two days.

On 30th of June, the Council of Europe (CoE) will organize a separate hub event connected to the main topic of the Forum, with expected participation from several international organizations.

Here below is the proposed agenda.

Day 1 – 28 June 2021

GMT	SESSION 1: Cybercrime policies and legislative updates in Africa
09h00	<p>High-level welcome and opening remarks</p> <ul style="list-style-type: none"> • Dr Hilde HARDEMAN, Head of the European Commission's Service for Foreign Policy Instruments (FPI) • Alexander SEGER, Head of the Cybercrime Division of the Council of Europe and Executive Secretary of the Cybercrime Convention Committee (T-CY) • Baroness Beeban Tania KIDRON, Member of the House of Lords, Parliament of the United Kingdom • H.E. Amani ABOU-ZEID, Commissioner I&E, African Union Commission (AUC) <p>Session moderated by Moses Bayingana – acting Head of Division of ISD</p>
09h15	<p>Setting the scene and goals of the event</p> <ul style="list-style-type: none"> • Abdul-Hakeem AJIJOLA, Chair of AUCSEG
09h20	<p>Cybercrime legislation in Africa – Relevant updates</p> <ul style="list-style-type: none"> • Amabélia CHUQUELA, Coordinator of the Specialized Department for the Criminal Area, Attorney General 's Office, Mozambique • Mabahig Habib ELGADI, Senior Legal Counsel, Ministry of Justice, Sudan <p>Session moderated by AUCSEG (Justice John Ubena) and CoE (Catalina Stroe)</p> <p>Q&A session facilitated by AUC – AUCSEG and CoE</p>
10h00	<p>Policing Cybercrime and Protecting Human Rights in Africa – Ensuring an Appropriate Balance through Policies and Legislation</p> <ul style="list-style-type: none"> • Dr Nnenna IFEANY-AJUFO, Nigeria and AUCSEG <p>Q&A session facilitated by AUC – AUCSEG (Dr Janvier NNGOULAYE) and CoE (Catalina Stroe)</p>
10h30	Health break
10h45	<p>Cyber security and cybercrime policy updates</p> <ul style="list-style-type: none"> • Dr. Raphael KOFFI, Ag. Director, Digital Economy & Post, ECOWAS Commission • Dr. Albert ANTWI-BOASIAKO, National Cybersecurity Advisor, Ghana • Ouanilo MEDEGAN FAGLA, General Director, Agence Nationale de la Sécurité des Systèmes d'Information, Bénin • Aymen AOUIINI, Colonel Major, Head of Cyber Secret Unit, Ministry of the Interior, Tunisia <p>Q&A session facilitated by OCWAR-C (Hein Dries)</p>

11h15	<p>Lack of data protection legislation: An enabler of Cyber Crime</p> <ul style="list-style-type: none"> • Michael ILISHEBO, Zambia • Prof Sizwe Snail ka Mtuze, Director - Snail Attorneys, South Africa <p>Q&A session facilitated by AUC</p>
11h45	<p>Data protection legislation as enabling factor for digital innovation plans</p> <ul style="list-style-type: none"> • Irene KABUA, Principal Legal Officer, Law Reform Commission, Kenya • Sanusi DRAMMEH, Principal ICT Officer, Ministry of Information & Communication Infrastructure, The Gambia <p>Q&A session facilitated by AUC (Mihret Woodmatas)</p>
12h15	<p>Key takeaways of day 1</p> <ul style="list-style-type: none"> • African Union Commission • Council of Europe
12h30	End of Day 1

**interventions to be Confirmed*

Day 2 – 29 June 2021

GMT	SESSION 2: International cooperation on cybercrime and e-evidence
09h00	<p>Policing and prosecuting cybercrime through international cooperation: Prospects and Challenges</p> <ul style="list-style-type: none"> • T. George-Maria TYENDEZWA, Assistant Director, Federal Ministry of Justice, Nigeria, Vice-Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes • Janvier NNGOULAYE, AUCSEG <p>Session moderated by AUCSEG – Jean-Robert Hountomey</p> <p>Q&A session facilitated by the AUC</p>
09h45	Health break
10h00	<p>Policing and prosecuting cybercrime through international cooperation: Online child safety</p> <ul style="list-style-type: none"> • Dr Sherif HASHEM, AUCSEG • Dr Towela JERE, Head, Economic Integration Division, NEPAD • Nina LICHTNER, Council of Europe <p>Session moderated by AUC – Adil SULIEMAN</p> <p>Q&A session facilitated by the AUC</p>
11h00	<p>Enhanced cooperation on cybercrime and electronic evidence – the Second Additional Protocol to the Budapest Convention</p> <ul style="list-style-type: none"> • Papa Assane TOURE, Magistrate, Deputy General Secretary of the Government, Senegal • Alexander SEGER, Head of the Cybercrime Division of the Council of Europe and Executive Secretary of the Cybercrime Convention Committee (T-CY) <p>Q&A session facilitated by the CoE (Nina LICHTNER)</p>
11h45	<p>Creating synergies for a coordinated approach to capacity building in Africa</p> <ul style="list-style-type: none"> • Panel with international organizations (expected: AUC, INTERPOL, CoE, UNODC, U.S. DoJ, ComSec) <p>Facilitated by the GFCE - César Moliné</p>
12h30	<p>Panel on the way ahead – Recommendations from the Second African Forum on Cybercrime</p> <ul style="list-style-type: none"> • Abdul-Hakeem AJIJOLA, Chair of AUCSEG • Alexander SEGER, Head of the Cybercrime Division of the Council of Europe and Executive Secretary of the Cybercrime Convention Committee (T-CY) <p>Moderated by the AUC</p>

13h00

End of Conference

**interventions to be confirmed*

Contacts

At the African Union Commission:

Adil SULIEMAN

Senior Policy Officer, Telecom and ICT
Department of Infrastructure and Energy,
African Union Commission
Email: Suliemana@africa-union.org

In the Council of Europe:

Catalina STROE

Programme Manager
Cybercrime Programme Office of
the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 78 30
Email: Catalina.stroe@coe.int

Nina LICHTNER

Cybercrime Programme Office of
the Council of Europe (C-PROC)
Bucharest, Romania
Email: Nina.LICHTNER@coe.int