

Regional exercise on the cooperation through the 24/7 Network established under the Convention on Cybercrime for Africa

26 November 2025, in Nairobi, Kenya

Supported by the GLACY-e, CyberSouth+ and Octopus projects

Outline

Background and justification

Offences involving computers have grown rapidly both in number and in sophistication, impacting countries and communities at all levels and posing a threat to human rights, democracy and rule of law. However, there has been a time lag in responding to these challenges by developing effective legislation and capacities for the criminal justice authorities as part of the process for aligning strategies and policies in a consistent and harmonized manner.

The cross-border nature and transversal implication of cybercrimes and electronic evidence present significant challenges to the law enforcement authorities, when carrying out such investigations that require a level of specialization and tools for international cooperation. Moreover, the development of the technology and its use in everyday life has also increased the number of criminal cases where electronic evidence is present. The cloud computing technology offers opportunities for expanding the business but at the same time brings new challenges to criminal justice authorities in the process of getting access to electronic evidence from foreign jurisdictions. In this context, suitable legal provisions are needed to facilitate cross-country investigations on cybercrime and international cooperation for the exchange of electronic evidence.

In view of responding to countries' capacity-building needs on cybercrime, the Council of Europe through its legal international standards such as [Convention on Cybercrime \(Budapest Convention\)](#), and the [Second Additional Protocol](#) offers tools for criminalization of conducts, procedural powers to be used in investigations and prosecutions as well as a mechanism for international cooperation.

In respect to international cooperation, the Budapest Convention provides several mechanisms such as the 24/7 Network established based on the Article 35, requiring to its members to be available on a permanent basis, to ensure expedited cooperation for the purpose of criminal investigations or proceedings involving the collection of evidence in electronic forms. The responsibilities of the 24/7 Network are to be further expanded under the framework of the Second Additional Protocol, particularly in the context of requests for expedited disclosure of stored computer data in an emergency (Article 9) and emergency mutual legal assistance (Article 10).

A number of countries from Africa have become Parties to the Convention and are now expected to be able to engage in international cooperation, including through their national 24/7 contact points. In support of the setting up of the 24/7 point of contacts in these countries, the Secretariat of the Network in cooperation with the [Cybercrime Programme Office of the Council of Europe](#) has provided the

necessary guidance on the organization and functioning of the national contact points. Moreover, the practices and experiences of other countries were shared for a better understanding of the challenges faced in the cooperation and the necessary resources to be allocated.

The Council of Europe will organise a 1-day regional event on the cooperation through the 24/7 Network for the Parties and Observers from Africa. The event will be a blend of practical (case simulation exercise) and theoretical aspects in view of enhancing the cooperation through the 24/7 Network.

The activity will be carried out as a side event of the African Forum on Cybercrime to be held in Kenya, on 25-27 of November. The Forum will focus on addressing emerging threats and identifying more effective ways to counter cybercrime as well as to serve as a platform for exchanging knowledge and practical experience based on successful operations.

Expected outcome

The regional exercise aims to provide the participants with a real case scenario on the functioning of the 24/7 Network. It will be followed by discussions on the challenges derived from the establishment of 24/7 POC, as well as the required capacities and capabilities for its functioning based on the good practices from other members.

By the end of the workshop, it is expected to have:

- increased knowledge on the role and functioning of the 24/7 Network
- enhanced the cooperation through this channel
- better understanding on where to place the 24/7 contact point in the countries in the process of acceding to the Budapest Convention.

Participants

The workshop is envisaged for representatives of the 24/7 POC from Benin, Cabo Verde, Cameroon, Côte d'Ivoire, Ghana, Mauritius, Morocco, Nigeria, Rwanda, Sao Tome and Principe, Senegal, Sierra Leone and Tunisia. In addition, representatives of law enforcement, prosecution service or other relevant institutions from Kenya, Malawi, Mozambique and Seychelles (as Observer States) will be invited.

Administrative arrangements and location

The workshop will take place in Nairobi, Kenya at a selected venue to be communicated at a later stage. The Council of Europe will fund the participation of up to 2 delegates representing the 24/7 POC, law enforcement, prosecution service or other relevant institutions from the countries indicated above.

The language of the event will be English and simultaneous interpretation in French will be provided.

Agenda

Kenya time	25 November – Regional exercise
09h00	Opening remarks <ul style="list-style-type: none"> Kenyan authorities Secretariat of the 24/7 Network, Council of Europe
09h15	Introduction of the participants – Tour de table <ul style="list-style-type: none"> Each delegate is expected to briefly introduce the experience of its 24/7 contact point and expectations from the workshop
9h45	Role and responsibilities of the 24/7 Network <ul style="list-style-type: none"> Secretariat of the Network 24/7 contact point of France (TBC)
10h45	<i>Coffee break</i>
11h15	Practical exercise on preservation of data (group work) <ul style="list-style-type: none"> Categories of data Format and content of the request Approval and execution of the request Channels for submission of the request MLA process for access to data
12h15	Feedback on group work
13h00	<i>Lunch break</i>
14h00	Practical exercise on additional responsibilities of the 24/7 Network (group work) <ul style="list-style-type: none"> Technical advice Legal information Collection of evidence
14h45	Feedback on group work
15h30	<i>Coffee break</i>
16h00	Capacities and resources for 24/7 contact point (Templates and Standard Operating Procedures) <ul style="list-style-type: none"> Secretariat of the Network 24/7 contact point of France (TBC)
17h00	Conclusions and take aways

Contacts

At the **COUNCIL OF EUROPE:**

Virgil SPIRIDON

Head of Operations
Cybercrime Programme Office of
the Council of Europe (C-PROC)
Bucharest, ROMANIA
Virgil.SPIRIDON@coe.int

In Kenya

James KIMUYU

Director National Computer and Cybercrime
Coordination Committee (NC4), Kenya
Email: jjkimuyu@nc4.go.ke