AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

THE AFRICAN UNION MECHANISM FOR POLICE COOPERATION (AFRIPOL)
NATIONAL ROAD, N° 36BEN AKNOUN ALGIERS, ALGERIA, P.O. BOX 61 BIS TEL: 213 23 38 43 56 FAX: 213 23 38 43 58
Website :https://afripol.africa-union.org /Email: afripol@africa-union.org

AFRIPOL CYBERCRIME STRATEGY

Table of Contents

1. INTRODUCTION

Cybercrime isone of the most rapidlydevelopingoffencesamong the fastest growing forms of transnational crime facing Member States of the African Union.

The rapid development of the Internet and information technology has boosted economic and social growth, but the increasing dependence on the Internet has also created risks and vulnerabilities, as it opened new possibilities for criminal activity.

Since cybercrime knows no borders, law enforcement agencies struggle to provide an effective response because oflimitations inherent in cross-border investigations, legal challenges, and disparities in state-to-state capacities.

Unlike in other investigations, in many cases of cybercrime, the digital evidence is held primarily by the private sector which manages and maintains several pieces of the Internet's infrastructure. Consequently, it isessential to establish collaboration among numerous actors to fight modern cyberthreats.

AFRIPOL's Cybercrime Strategy presents the plan which will be drawn up to help its Member States combat cybercrime through coordination and development of specialised police capacities during the period 2020-2024.

The Strategy is a flexible document, which will be reviewed periodically to ensure that it remains relevant, that it continues to respond to emerging threats in the dynamic environment in which the security forces operate, and that it meets Member States'expectations. This documentprimarily seeks to draw the road map for fighting cybercrime, that is, the main lines of action for developing control measures for offences that target computers and information systems, in attempts to gain unauthorized access to devices or to prevent legitimate users from accessing those devices (often using malware).

This strategy revolves around four lines of action with a common objective to help States develop coherent control methodologies and thus ensure a fruitful exchange of information.

These lines of action are to:

i. Strengthen the capacities of AFRIPOL's central cybercrime team, as well as of Member States' teams, by providing resources and mechanisms for collection of the evidence necessary for digital investigations.

ii. Strengthen the capacities of Member States through specialised training in fighting cybercrime.

iii. Developharmonious and coherent regulation, as well as extensive cooperation among Member States of the African Union.

iv. Ensureperpetualthreat assessment, in respect of cybercrime at the continental level.

2. PURPOSE OF THE STRATEGY

AFRIPOL provides support to the police institutions of its 55 Member Statesby helping them to share resources and skills for identifying clues and intelligence, to provide the missing information and to dismantle organized networks that are at the root of various often interrelatedcybercrime acts.

To this end, AFRIPOL is developing a strategy to fight cybercrime, which is entirely consistent with the Strategic WorkPlan (2020-2024). This Strategy acknowledges the importance of collaborative efforts with various initiatives to combat all forms of crime to ensure consistency and effectiveness in the approach to combattransnational crime and to tackle all dimensions of the problem.

Thanks to its cybercrime strategy, AFRIPOL confirms its role as an information-sharing platform, operational coordinator, and facilitator of national, regional, and international initiatives to fight cyber threats on the African continent and in close coordination with international organizations that are active in this field. AFRIPOL harmonizes practices in the various initiatives to combat cybercrime and compares them to international best practices, in a bid to ensure their optimal effectiveness. Consequently, AFRIPOL establishes robust partnerships between the various actors in the fight against cybercrime.

The exchange platform that AFRIPOL intends to set up to fightcybercrime in Africa will help to consolidate the efforts of the 55 Member States of the African Union and concurrently assist the security forces of these same States to develop harmonious legislation that facilitates information exchange and expertise sharing across the continent.

This legislative and regulatory support will be accompanied by technical support, which will be reflected in training and cooperation actions, in a bid to build the capacities of cybercrime cells of the police forces of States of the African Unionin fighting cybercrime.

AFRIPOL will act as a relay and focal point in this field to simplify exchanges and create bridges that permit inputs to be made by identified experts and by centres of excellence that will be established. Thus, all initiatives registered in this field will converge.

3. STAKEHOLDER ANALYSIS

This Strategy, though providing a framework for AFRIPOL's action to improve the response of law enforcement agencies fighting this form of crime, also includes, among others, support and capacity building for fighting cybercrime for the existing regional police cooperation organisations, with the East Africa Police Chiefs Cooperation Organisation (EAPCCO), the Central African Police Chiefs' Committee (CAPCCO), the West AfricanPolice Chiefs Committee (WAPCCO), and the Southern African Regional Police Chiefs Cooperation Organization (SARPCCO) providing a continental cooperation framework at the strategic, operational and tactical levels to fight cybercrime in Africa.

It will also strengthen cooperation by identifying common information gaps and sharing important information that is vitalto AFRIPOL's effectiveness in combating cybercrime on the Continent. It should be noted that the Agreement between the African Union and the International Criminal Police Organization (INTERPOL) in relation to the cooperation between INTERPOL and the African Union Mechanism for Police Cooperation (AFRIPOL) provides for interoperability between the African Police Communication (AFSECOM) system of AFRIPOL and the I-24/7 communication system of INTERPOL as an essential tool for cooperation between the two organisations, and the ISPA (INTERPOL Support Program for the African Union) project developed in this context provides a pillar dedicated to this theme.

4. STRATEGIC PRIORITIES IN CYBERCRIME

This Strategy revolves around four (4) essential areasthat will help AFRIPOL, its Member States and the stakeholders involved to advance towards the realization of the vision of a more secure cyberspace at the continental and international level.

Strategic Priority 1: Strengthen the capacities of AFRIPOL's central cybercrime team, as well as of Member States' teams, by providing resources and mechanisms for collection of the evidence necessary for digital investigations.

- StrengthenAFRIPOL'scentral team by increasing human and material resources.

- Standardise procedures for digital investigation and information collection to inculcate the concept of digital evidence.
- Homogenise the hardware and software in use, and which are specific to this process.
- Develop reference guides for applying techniques and protocols that respect legal procedures and are intended to provide digital evidence in response to requests from judicial-type institutions made by requisition or court order.
- Makeavailable to Member States all knowledge and methods for collection, storage,and analysis of evidence from digital media with a view to producing them in the context of legal proceedings.
- AssistMember States to setup digital forensic laboratories where digital investigations will be conducted, and the digital evidence acquired will be stored. The laboratorieswill contain sets of hardware and software tools that help investigators to acquire and analyse digital evidence and to present their results in formal reports.

StrategicPriority 2: Strengthen the capacities of Member States through specialised training in fighting cybercrime.

- Plan basic and advanced training sessions according to the level of investigators from Member States involved in fighting this form of crime.
- Facilitate workshops on the chain of custody during cybercrime investigations, in terms of obtaining and interpreting digital evidence and clues.
- Facilitate workshops on cybercrime investigative methods as part of joint investigations conducted at the regional, continental, or international level.
- Conduct training and exchange workshops with experts from Member States on potential new threats and ensure the disseminationof such information.
- Putting E-Learning type training courses online on the AFRIPOL E-Learning platform hosted by the African Union.
- Identify and strengthen cooperation with centres of excellence specialising in Cybercrime in Africa.
- Develop training manuals, guides and best practices for distribution to Member States.
- Develop and deploy generic and tailor-made training programmes for strengthening police cooperation in fighting cybercrime in Africa.

Strategic Priority 3: Develop harmonious and coherent regulation, as well as extensive cooperation among the Member States of the African Union.

- Maintain exchanges through the establishment of working groups which bring together experts from member countries.
- Coordinate, at the continental and global level, the operational and tactical action of the main actors involved in fighting cybercrime.
- Build bridges between law enforcement agencies, the public sector, the private sector, academia, research bodies, international organisations, and other entities.
- Strengthen public-private partnerships and collaborate to maximize the impact of operational action.
- Assist police institutions of Member States to strengthen cooperation frameworks at national, regional, continental, and international levels.
- Represent law enforcement agencies of Member States on international bodies that define the future of the Internet or which have an influence on it, for example, the International Telecommunications Union (ITU) and the Internet Corporation for Assigned Names and Numbers (ICANN).
- Coordinate and carry out joint actions within the scope of the fight against cybercrime, in partnership with the International Criminal Police Organization(INTERPOL), the United Nations Office on Drugs and Crime (UNODC) and other continental bodies, in Europe, namely, the European Union's law enforcement agency (EUROPOL*),* the European Union Agency for Law Enforcement Training (CEPOL), or, in Asia (Asiapol), or in South America (Americapol) and others.
- Enable the extension of the operational scope of law enforcement agencieswhile ensuring the interoperability of their actions.
- Ensure that the African Union Convention on Cyber Security and Personal DataProtection, which was adopted by the Assembly of the African Union at its 23rd Ordinary Session held in June 2014, in Malabo, Equatorial Guinea, is amended to include a section specific to cybercrime.
- Assist Member States to improve and harmonise legal frameworks for fighting cybercrime.
- Enhance the interoperability of law enforcement agencies and other stakeholders, by adopting homogenous communication channels and reporting formats.
- Strengthen cooperation in fighting cybercrime by mobilizing experts identified on the African continent to respond to requests for assistance expressed by Member States.

Strategic Priority 4: Ensure perpetual threat assessment, in respect of cybercrime at the continental level.

- Develop actionable cybercrime intelligence and alerts through a multi-stakeholder approach.
- Help law enforcement agencies to gain more knowledge about cybercrime trends.
- Use existing bridges with the public and private sectors to learn about current and future threats and trends andshare their expertise and best practices.
- Ensure constant monitoring of threats by preparing maps of risks and attacks, by adopting an alert dissemination system.

5. MONITORING AND REPORTING

In accordance with the provisions of Article 8of AFRIPOL's Statutes on the General Assembly, the Work Plan shall be submitted to the General Assembly for consideration.

It should be noted that reports shall be drawn up to enable regular monitoring and evaluation of the implementation of this Work Plan.

6. CONCLUSION

While most crimes are circumscribed by borders, cybercrimesare still the only form of crime with virtually no border restrictions.

AFRIPOL, as the African Union’smechanism for police cooperation, through this Strategy, seeks to put in place the first brick in the common fight against this form of criminality and to converge all efforts to ensure the coherence of operational action, while strengthening law enforcement agencies to bring them to a uniform level of expertise and know-how.

The AFRIPOL Strategy will undoubtedly permit all Member States to benefit from each other's experience, while creating horizontal and vertical bridges with identified public or private actors, engaged in fighting this form of transnational crime.

However, this strategy remains flexible and subject to periodic review to ensure that it remains relevant andconsiderspotential new threats existing in the dynamic environment in which security forces operate.