#3AFcybercrime

Key Messages

Third African Forum on Cybercrime and Electronic Evidence

Strengthening Africa's response to cybercrime

Nairobi, Kenya | 25 - 27 November 2025

More than 350 cybercrime experts from over 31 African countries, representing criminal justice authorities, cybersecurity actors, data-protection authorities, academia, civil society and the private sector, converged in Nairobi from 25–27 November 2025 for the Third African Forum on Cybercrime and Electronic Evidence.

> *The strategic significance of this Forum goes beyond operational deliverables: it is an opportunity to reshape how Africa secures its digital future. A coordinated regional posture reduces criminal safe havens, strengthens cross-border digital trade and enhance global resilience against sophisticated threats. It is an opportunity to pool technical expertise, law enforcement capacity as well as work together to deliver the vision of a secure digital space.*
>
> **William KABOGO GITAU**, Cabinet Secretary, Ministry of Information, Communications and the Digital Economy of Kenya

> *"We are running a real risk of a generation exposed to identity theft, misinformation, exploitation, and manipulation on an unprecedented scale."*
>
> **Dr. Raymond OMOLLO**, PhD, Principal Secretary for the State Department for Internal Security & National Administration, Kenya.

#3AFcybercrime

Key Messages

The Forum counted on attendance of members of the Kenyan Government such as the Cabinet Secretary for ICT and Digital Economy William KABOGO GITAU, the Principal Secretary for the State Department for Internal Security and National Administration Raymond OMOLLO, the Director General of the Judiciary Academy Smokin WANJALA and top representatives from the Council of Europe, European Union, INTERPOL, United Nations Office for Drugs and Crime (UNODC) and other international partners. This gathering of diverse and senior stakeholders underscores an unprecedented continental commitment to consolidating Africa's cyber-crime resilience and advancing cross-border cooperation.

"These threats are borderless. A cyber incident originating thousands of miles away can destabilise institutions here at home within seconds if not minutes. This makes one point undeniable, that our response must be coordinated, international and sustained. We must be able to strengthen our collective capacity to detect, deter and prosecute cyberthreats while safeguarding the integrity of digital platforms across our borders."

Dr. Raymond OMOLLO, PhD, Principal Secretary for the State Department for Internal Security & National Administration, Kenya.

Across Africa, the momentum to build a safer and more resilient digital environment has never been stronger. Governments are demonstrating increasing political will to modernise legislation, invest in specialised capabilities and align national frameworks with global standards. This collective energy presents a clear message: the time is now to translate political commitment into concrete, harmonised and sustainable cybercrime action. Kenya's leadership, reflected in its strong Governmental engagement and its commitment to regional cooperation, embodies this turning point. Supported by high-level representatives and experts from across the continent, the African cyber ecosystem is engaged to advance a coherent and strong response to cybercrime.

"The fight against cybercrime requires sustained action across borders, across institutions. This forum embodies exactly that spirit."

Matthias Kloth, Head of Digital Governance and Sport Department of the Council of Europe

"Cybercrime has become transnational and highly complex. Investigators and prosecutors must adapt rapidly to protect citizens and uphold the rule of law."

Vinsent Perera, Attorney General of Seychelles

The following key messages emerged from the Third African Forum on Cybercrime and Electronic Evidence:

#3AFcybercrime

Key Messages

Workshop #1: Cybercrime legislation in Africa and international standards

Effective **cybercrime legislation** combines legal clarity, operational practicality, and human-rights safeguards. Defining offences that reflect contemporary criminal techniques, alongside procedural powers enabling timely access to electronic evidence, equip authorities with a robust enforcement toolkit. Embedding judicial oversight ensures that investigative measures remain compatible with constitutional and human-rights standards. When national frameworks align with internationally recognised standards, countries gain legal certainty, strengthen cross-border cooperation, improve prosecutorial outcomes, and foster trust among international partners. The framework of the Budapest Convention on Cybercrime remains the more stable and exercised one and in complementarity with Malabo Convention and Hanoi Convention provide African countries the relevant international standards for harmonisation of their domestic legislation.

More details here.

Workshop #2: Cybercrime threats and trends

Africa's **cybercrime landscape** is shaped by professionalised criminal networks, commoditised tools and scalable cybercrime-as-a-service offerings that are exploiting advances in artificial intelligence. Emerging threats, including online scams, ransomware, business email compromise, SIM fraud, digital extortion and cryptocurrency-enabled laundering, highlight the need for advanced early-warning systems and behavioural-analysis capabilities. Streamlining structured information flows among cybersecurity actors, law enforcement, financial institutions and on-line service providers enables faster disruption, more accurate attribution and greater resilience against rapidly evolving cyber threats. Effective responses rely on combining necessary knowledge, technical, operational and legal capacities, underpinned by international cooperation instruments for access to data from foreign jurisdictions.

More details here.

#3AFcybercrime

Key Messages

Workshop #3: Follow the money: tracing and seizing illicit financial flows and virtual assets

Illicit Financial Flows & Virtual Assets. Cryptocurrencies, while offering significant opportunities for innovation and financial inclusion, are increasingly exploited for investment scams, ransomware payments, illicit marketplaces, sanctions evasion, and cross-border laundering. Key challenges in addressing illegal use of virtual assets include regulatory gaps, limited cooperation of some virtual asset service providers, the use of privacy-enhancing technologies, and insufficient technical expertise. Responses require increasing stakeholder understanding of crypto, building technical and investigative capacity, and fostering international cooperation. Initiatives such as the Africa Cryptocurrency Working Group illustrate how regional collaboration can strengthen training, resource sharing in a coordinated action. In the absence of specific laws, investigators and prosecutors can adopt creative approaches by using the existing legislative framework to move forward with their cases. Effective solutions include reinforced legislation, strengthened KYC/AML controls, specialised training, public-private partnerships, and close coordination between criminal justice actors.

More details here.

Workshop #4: Role of policymakers and legislators in the fight against cybercrime: when policy meets practice

Policymaking and their legislative roles. Legislators are not just lawmakers but strategic partners in the fight against cybercrime. They also ensure proper resources and funding to enable criminal justice authorities to properly pursue justice. Laws must keep pace with technology. Cybercrime evolves at digital speed and legislators have a critical responsibility to ensure laws are agile, technology-neutral, and time- proofed for years to come. Moreover, clear and precise legal terminology and predictability in laws instruct criminal justice authorities in fair application of the law, reducing the risk of arbitrary enforcement and abuse. Proper checks and balances in cybercrime laws build trust and public confidence in their representatives and in the state's capability and capacity to protect its citizens.

More details here.

#3AFcybercrime

Key Messages

Workshop #5: Impact of artificial intelligence on cybercrime

Emerging technologies such as **Artificial Intelligence (AI)**, offer significant opportunities for cybercrime investigations, from advanced pattern recognition to automated triage, while generating novel forms of evidence. Ensuring their responsible and effective use requires transparent methodologies, explainable outputs and safeguards that promote fairness and prevent bias. The Budapest Convention framework provides a robust legal foundation for addressing cybercrime, and its provisions can be effectively applied to AI-related contexts such as verifying authenticity, managing synthetic content and supporting secure digital processes. Engaging service providers as strategic partners brings operational expertise, threat intelligence analysis, and technical support, improving collaborative capacity-building initiatives, especially in African countries. By harnessing synergies between AI-driven investigative tools, international legal standards, including the Council of Europe's new Framework Convention on AI, and these multi-stakeholder partnerships, empower criminal justice actors to respond effectively and confidently to emerging cybercrime threats.

More details here.

Workshop #6: Electronic evidence: chain of custody and admissibility

Electronic Evidence and Chain of Custody. Safeguarding integrity and reliability is essential to ensure admissibility of evidence in court. It requires strong cooperation across the entire justice chain. Investigators, digital forensics experts, prosecutors, and judges face distinct challenges. Yet all emphasized the need for proper knowledge, early coordination and clear communication to prevent gaps in the chain of custody. Electronic evidence is now central not only to cybercrime cases, but to virtually all forms of crime, making whole-of-system collaboration essential. Strengthening legal frameworks, complemented by harmonized Standard Operating Procedures, along with building technical and judicial capacity across Africa are priorities to ensure that countries can effectively request and use electronic evidence in cross-border cases. International cooperation frameworks and standards - such as those outlined in the Budapest Convention are important reference points for guiding these efforts.

More details here.

#3AFcybercrime

Key Messages

Workshop #7: Data protection as an enabler for international cooperation on cybercrime

Data protection is a core enabler of lawful, secure, and trustworthy international cooperation on cybercrime and electronic evidence. As digital evidence becomes increasingly complex and transnational, legal frameworks must ensure clear safeguards, strong oversight, and interoperable procedures that support timely information exchange. Upholding high standards of transparency, security, and accountability is essential to protecting rights and maintaining investigative integrity. Aligning national laws with instruments such as the Malabo Convention and Convention 108+, reinforcing supervisory authorities, and embedding privacy-by-design across digital systems are key to facilitating reliable cross-border cooperation. These commitments are essential for building the trust and resilience needed to combat cybercrime effectively across the continent.

More details here.

Workshop #8: Cybercrime capacity building: sustainable training

Cybercrime capacity building is a key enabler to enhance knowledge, competencies and skills of all actors across society in the digital age. This also calls for international and regional actors working in this field to join forces and effectively exploit the synergies between different programs to avoid overlaps and streamline resources. Regional training centers play a crucial role in reducing fragmentation, strengthening the harmonization of practices and support for essential judicial cooperation. Sustaining a focus on gender-sensitive approaches within the traditionally male dominated field of cybercrime investigations is a must. Both countries and implementers should ensure that gender doesn't become a 'box-ticking' exercise in the capacity building efforts. Equally, youth should be involved in programmes addressing capacity building needs from the designing phase, as future owners of the project, to plan for transfer, adapt content, and ensure sustainability.

More details here.

#3AFcybercrime

Key Messages

Workshop #9: International cooperation on cybercrime and electronic evidence: the Second Protocol to the Budapest Convention on Cybercrime

Second Additional Protocol to the Budapest Convention. No single country can address the complexity of electronic evidence alone. Instruments such as the Budapest Convention and its Second Additional Protocol provide the legal basis needed for enhanced international cooperation, particularly with service providers, under strong human rights and rule of law safeguards. The Protocol, in particular, is a unique instrument offering faster procedures for obtaining subscriber information, clearer and more reliable channels for cooperation with service providers and reinforced mechanisms for emergency situations. Effective implementation of the Protocol requires time for carefully planned reforms, including updating legislation, strengthening institutional structures, improving coordination among authorities, and ensuring robust data-protection safeguards. The Cybercrime Programme Office of the Council of Europe (C-PROC), stands ready to support countries in this endeavour through dedicated capacity building activities.

More details here.

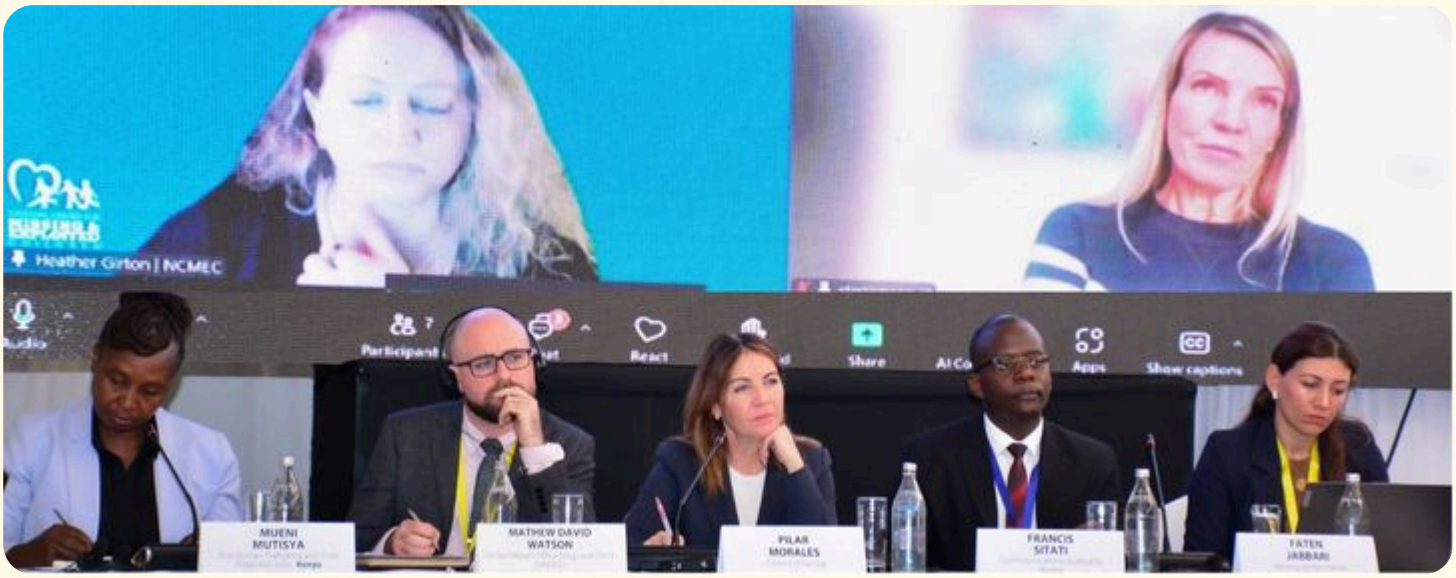
Workshop #10: Policies and strategies on cybersecurity and cybercrime

National strategies on **cybersecurity and cybercrime** in Africa are most effective when they integrate cybersecurity governance, incident response, criminal-justice capabilities and regulatory oversight into a coherent continental and national framework. Coordination across public entities, private-sector actors, civil society and technical communities ensures that prevention, detection and enforcement complement each other. Private actors play a critical role by contributing with operational expertise, threat intelligence and technical support, complementing legal frameworks and strengthening investigative and prosecutorial capacities across the African continent. Effective strategies prioritise transparent reporting mechanisms, early-warning systems and clear institutional mandates, encourage responsible disclosure while building a culture of digital trust. By leveraging these synergies within structured capacity-building initiatives, African states are better equipped to respond efficiently and confidently to evolving cyber threats, while ensuring alignment with international standards and respect to human rights.

More details here.

#3AFcybercrime

Key Messages



Workshop #11: Child protection online and cyberviolence

Fighting against **online child sexual exploitation and abuse** demands legal frameworks that are not only aligned with international standards but fully operationalised in daily practice. Effective responses rely on clear reporting pathways, the structured use of tools such as CyberTipline information, robust triage systems, and integrated workflows that link digital forensics, victim identification, and inter-agency coordination. States must reinforce specialised police units with sustained resources, modern investigative capabilities, and child-centred protocols that safeguard survivors' protection and privacy. At the same time, stronger cooperation with digital platforms – through timely data access, proactive safety measures for minors, and disruption of organised criminal networks – is essential to counter rapidly evolving tactics. This work also benefits from stronger North–South cooperation, supported by the Council of Europe's North-South Centre, which helps countries share experiences and coordinate efforts across regions. By combining legislative clarity, institutional capacity, and cross-sector partnerships, countries can build coherent and effective systems that ensure children are better protected from online victimization.

More details here.

Workshop #12 Ransomware attacks: legislation, prosecution and investigative tools

Ransomware Response. The African region faces a critical ransomware threat, with annual losses nearing $3 billion, driven by R-A-A-S models and AI-enhanced social engineering that employs double extortion and targets critical infrastructure via unpatched systems. Effective countermeasures are undermined by the tension between cybersecurity entities prioritizing recovery and law enforcement focusing on identification of the source and traces, compounded by significant investigative delays, crime scene destruction, and challenging international cooperation due to slow instruments and complex virtual asset tracing. To strengthen defence, organizations must commit to the "Do Not Pay the Ransom" policy, ensure immediate isolation and reporting to law enforcement to preserve the crime scene, and institutionalize regular simulation exercises to align response actions. Ultimately, mandatory implementation of technical training, robust backup strategies, and comprehensive disaster recovery plans are essential to build resilience against these threats.

More details here.

#3AFcybercrime

Key Messages

Workshop #13: Cybercrime and human rights: the case of the freedom of expression

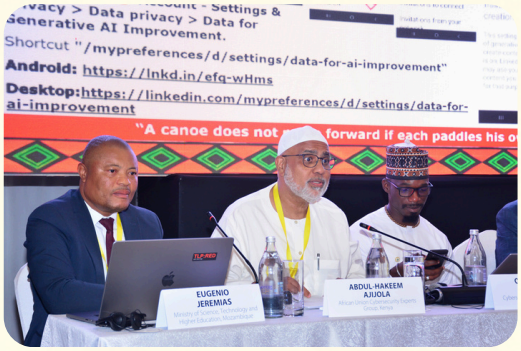
Cybercrime & Human Rights. Freedom of expression remains a cornerstone of societies committed to fundamental rights. At the same time, some cybercrime laws, particularly those that are broadly worded or vague, can inadvertently restrict this fundamental right. Judges often find themselves interpreting such laws, and it is essential to do so in a manner that is consistent and guided by human rights principles. Restrictions on speech, particularly online, should address substantial harm while avoiding unnecessary interference with public debate. Overly broad or vague cybercrime provisions risk overcriminalisation, creating uncertainty for citizens and criminal justice authorities, and underscore the importance of precise, clearly drafted legislation. Alternatives to criminal sanctions should be considered wherever possible. Addressing harm through civil remedies, or administrative measures may be more proportionate and less restrictive than criminal penalties, helping maintain trust in judiciary.

More details here.

#3AFcybercrime

Third African Forum on Cybercrime and Electronic Evidence

Strengthening Africa's response to cybercrime



With special thanks to the Government of Kenya,

HARAMBEE

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime