AFRICAN UNION الاتحاد الأفريقي UNIÓN AFRICANA		UNION AFRICAINE UNIÃO AFRICANA UMOJA WA AFRIKA

AFRICAN COURT ON HUMAN AND PEOPLES' RIGHTS
COUR AFRICAINE DES DROITS DE L'HOMME ET DES PEUPLES
P.O. Box 6274 Arusha, Tanzania – Telephone: +255 272 510 510
Website:www.african-court.org / Email: registrar@african-court.org

PRESENTATION BY HON. JUSTICE DUMISA B NTSEBEZA, JUDGE, AFRICAN COURT ON HUMAN AND PEOPLES' RIGHTS
AT THE J20 SUMMIT 2025 OF HEADS OF CONSTITUTIONAL COURTS AND SUPREME COURTS OF THE GROUP OF 20 MEMBERS.

THEME: JUSTICE IN A TIME OF CHANGE: INDEPENDENCE, INNOVATION AND CO-OPERATION.

SESSION 4: COMBATING CYBERCRIME: STRENGTHENING CROSS-BORDER JUDICIAL COOPERATION.

4 September 2025

Honourable Chairperson,
Distinguished Delegates,
Esteemed Colleagues,
Ladies and Gentlemen,

Good morning/ Good afternoon to you all and welcome to Johannesburg. I thank the moderator for the kind introduction. I also extend my appreciation to the panellists from the earlier sessions for their enriching and insightful contributions.

It is indeed an honour and privilege to join this distinguished gathering on behalf of the African Court on Human and Peoples' Rights. I bring you warm greetings from Arusha, the seat of our Court, where we are presently convened for our 78th Ordinary Session.

The theme of "*Combating Cybercrime: Strengthening Cross-Border Judicial Cooperation"* could not be more apt. We are living in a fast-evolving digital era where the world is increasingly reliant on technology. Technology has undoubtedly unlocked vast opportunities, but it has also exposed us to unprecedented risks. Our interconnected world has become a fertile ground for seamless criminal activity across borders, giving rise to a complex challenge-transnational cybercrime.

The UN Trade and Development (UNCTAD)[1] has reported that "Cybercrime is an escalating issue affecting nations across all levels of developments, impacting both consumers and businesses. The dynamic nature of cyber threats and the accompanying skills shortages pose significant challenges for law enforcement and judicial systems, especially concerning cross-border enforcement.

Cybercrime represents one of the most complex challenges of the digital age. It undermines the integrity of financial systems, jeopardizes national security, threatens democratic processes, and violates human rights including the rights to privacy and dignity of individuals across the globe.

The theme of the present panel is vast and multifaceted. However, in the next fifteen to twenty minutes, I will focus on five key issues:

1. General Understanding of the scope and nature of cybercrime.
2. The role of the judiciary in combating cybercrime.
3. Cross-border judicial cooperation in combating cybercrime.
4. Current trends and challenges in judicial cooperation.
5. Proposals for strengthening cross-border judicial cooperation.

1. General Understanding of Cybercrime

[1] https://unctad.org/page/cybercrime-legislation-worldwide

There is no single universally accepted definition of cybercrime, but it broadly refers to illegal activities that involve the use of computers, networks, or the internet to perpetrate or facilitate a crime. For example, the Council of Europe's Convention on Cybercrime[2] outlines offences related to computer systems and data, and the new UN Convention against Cybercrime aims to establish a global framework for defining and combating these crimes[3]. Cybercrime is not a single offence, but rather a spectrum of unlawful activities enabled by or directed against digital technology. We can distinguish at least three categories:

a) **Cyber-dependent crimes (Type I),** such as hacking, spread of virus or malware, ransomware, distributed denial-of-service attacks, i.e., the flooding of internet servers to take down network infrastructure or websites, piracy, phishing. These can only be committed using a computer, computer networks or other form of information communications technology (ICT).

b) **Cyber-enabled crimes (Type II),** like fraud, corporate espionage, extortion, human trafficking, money laundering, child exploitation/pornography, where digital platforms amplify traditional offences. Unlike cyber-dependent crimes, they can still be committed without the use of ICT/digital technologies.

c) **Cyber-facilitated harms** These include disinformation campaigns, cyberbullying, cyberstalking, social engineering, catfishing, non-consensual pornography also often referred to as “revenge porn”. In such instances, the perpetrator is using the digital platforms especially social media platforms as a platform to commit crime.

As technology continues to evolve, cybercrime is also growing, with criminals becoming increasingly sophisticated and resourceful. What makes cybercrime even more uniquely challenging is its ability to transcend borders, as it occurs in the borderless realm of

[2] https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf
[3] https://www.unodc.org/unodc/cybercrime/convention/home.html

cyberspace. A perpetrator may reside in one country, route their attack through servers in another, exploit vulnerabilities in a third, and ultimately target victims in yet another.

2. The Role of the Judiciary in combating cybercrime

The judiciary must ensure that cybercrime laws are properly interpreted, applied consistently, and adapted to the evolving realities of the digital age. While many states have enacted cybercrime statutes, their interpretation often raises novel questions, for example: What constitutes unlawful access? How can digital evidence be authenticated? How should we balance free expression with restrictions on harmful online speech?

Courts across the world have had to grapple with these issues, sometimes extending the reach of domestic law into the digital space when online conduct has cross-border effects. For example, Indian courts have ruled that mobile phones fall within the definition of "computers" under the Information Technology Act, ensuring that tampering with mobile software counts as a cybercrime offence.[4] In another case, the Court set out conditions for the transmission and admissibility of evidence obtained from encrypted platforms in cross-border criminal cases.[5]

Courts are guardians of fundamental rights. In combating cybercrime, states often resort to measures such as surveillance, interception of communications, or cross-border data sharing. These tools are sometimes indispensable in tracking cybercriminals but risk infringing on the rights to privacy, due process, and free expression.

Landmark rulings from the courts demonstrate how judiciaries act as checks on excessive state power. For example, the European Court of Human Rights has reaffirmed that cybercrime investigations must respect fundamental rights, ensuring that the fight against crime does not come at the expense of legality and human dignity.[6] The Court has thus

[4] Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anor
[5] Case C-670/22, M.N. (EncroChat) (CJEU, 2024)
[6] Benedik v. Slovenia (ECtHR, 2018); Trabajo Rueda v. Spain (ECtHR, 2017

reinforced the judiciary's gatekeeping role, ensuring that investigative powers in cyberspace are subject to proper judicial oversight.[7]

The judiciary also functions as a bridge between international commitments and domestic law. When states ratify conventions such as the Budapest Convention, the African Union's Malabo Convention, or the newly adopted UN Cybercrime Convention, it falls to courts to interpret and apply domestic statutes in harmony with these international obligations. Judicial interpretation, therefore, becomes the mechanism through which global commitments are translated into enforceable rights and duties at the national level.

Courts contribute to building predictability and fostering cooperation across borders. A well-reasoned judgment in one jurisdiction can inspire others, promoting convergence in how cybercrime cases are handled. This cross-pollination of jurisprudence helps harmonize global responses to cybercrime and strengthening judicial cooperation.

Courts reinforce obligations of both State and private entities in combating cybercrime. For example, **the Bulgarian** NAP Cyberattack Case (2019) illustrates this vital role. In this breach, hackers stole the personal data of about 70% of Bulgaria's population from the National Revenue Agency. While the criminal hacker was prosecuted, the Bulgarian Supreme Administrative Court held that the state agency itself was liable under the GDPR for failing to adopt adequate security measures. The ruling emphasized that data controllers whether public bodies or private companies cannot escape responsibility simply because a third party carried out the attack. By recognizing non-material damages such as distress and fear of identity theft, the judiciary underscored that cybersecurity is a legal obligation tied to human dignity and trust. This case demonstrates how courts can strengthen cyber resilience by ensuring accountability and setting higher security standards for all data controllers.

However, the role of the Courts is not that straightforward. Given the nature of cybercrime; its transnational reach, high level of sophistication, and reliance on constantly evolving

[7] *Trabajo Rueda v. Spain* (ECtHR), 2017.

technologies, the role of the judiciary in combating this form of crime is complex. Courts cannot work in isolation. Instead, they must collaborate with a number of stakeholders including law makers, investigators, prosecutors, experts in forensics, IT and even international partners to ensure justice is delivered.

Importantly, the role of the judiciary in combating cybercrime in the digital age is also an opportunity for progressive innovation to address emerging realities; Take the Philippines, for instance. They have established special cybercrimes office in the department of justice to handle all matters relating to international mutual assistance and extradition for cybercrime and cyber-related matters. It also acts as the focal agency in formulating and implementing law enforcement investigation and prosecution strategies in curbing cybercrime and cyber-related offenses nationwide.[8]

In India, the judiciary has embraced procedural modernization by allowing the submission of electronic evidence in courts, even when it is stored in cloud servers or foreign jurisdictions.[9] This is particularly important in financial fraud and online harassment cases, where digital evidence is often the only link to the crime.

These examples show that in combatting cybercrime, the judiciary's role cannot be limited to the traditional function of interpreting and applying laws. Instead, courts should now be at the forefront of shaping how legal systems respond to the digital age, including among others:

a) Institutionalizing specialized mechanisms for cybercrime;
b) Modernizing procedures to accommodate digital evidence;
c) Building technical capacity to understand digital forensics, encryption, and online evidence trails; and
d) Driving international cooperation by setting precedents that encourage cross-border collaboration.

[8] https://www.doj.gov.ph/office-of-cybercrime.html accessed 1 September 2025 at 16:20 EAT.
[9] See the Bharatiya Sakshya Adhiniyam Act, No.47 of 2023.

e) Identifying legislative gaps that require reform

In short, the judiciary is not just an arbiter of disputes in cybercrime cases. It is also an innovator, a collaborator, and a bridge between technology and justice. By adapting in these ways, courts help ensure that the law keeps pace with the digital era, protecting individuals while also upholding fairness and due process.

3. Cross-border judicial cooperation

Cybercrime frequently transcends national borders, making international cooperation essential. Effective investigation, prosecution, and adjudication often depends on collaboration between countries, law enforcement agencies, and judicial institutions, supported by legal frameworks, international conventions, directives, guidelines, and recommendations.

For instance, the ***EncroChat case (C-670/22, CJEU, 2024)*** illustrates the need for coordinated action: evidence from encrypted devices located in multiple countries had to be transmitted, authenticated, and admitted in a cross-border criminal investigation. Similarly, the **Bulgarian *NAP cyberattack (C-340/21, CJEU, 2023)*** highlighted how data breaches affecting millions of individuals can have implications across EU member states, requiring harmonized interpretation of General Data Protection Regulation (GDPR) obligations and coordinated enforcement.

Cross-border cooperation is not limited to procedural matters; it also involves training and capacity-building. Each actor in the justice system requires specialized skills to operate effectively in a globalized digital environment:

Legislators and judges need a thorough understanding of how proposed cyber laws interact with international obligations and cross-border investigations. Investigators require hands-on training in data recovery, encryption/decryption, and forensic analysis across jurisdictions. Prosecutors must be able to interpret digital evidence from multiple

sources and present it convincingly in court. Judges must assess the admissibility, reliability, and relevance of evidence gathered internationally, while understanding the technical context of cybercrime investigations.

When all stakeholders are properly trained and equipped, confidence in cross-border cooperation increases, the law is applied consistently, and enforcement against cybercrime becomes more effective. Without judicial cooperation, cybercriminals can exploit gaps between legal systems, while coordinated action ensures that justice keeps pace with technology.

4. Areas that require judicial cooperation in combating cybercrime.

One critical area is the extradition of cybercriminals. When suspects operate across multiple jurisdictions, transferring them for prosecution ensures accountability and prevents safe havens for criminal activity. For example, the ***EncroChat case (C-670/22, CJEU, 2024)*** involved the cross-border investigation of encrypted communications, where coordinated efforts between France, the Netherlands, and other EU states enabled arrests and extraditions of organized cybercrime actors.

Another key area is the mutual recognition and enforcement of court orders. Judicial systems must acknowledge foreign judgments, search warrants, and subpoenas to access digital evidence stored abroad. The ***Bulgarian NAP case (C-340/21, CJEU, 2023)*** illustrates this need, as the cyberattack exposed personal data affecting citizens across multiple EU states, highlighting the importance of harmonized GDPR interpretation and cross-border enforcement.

Cross-border data sharing and access to evidence is equally critical. Investigations often require access to logs, emails, cloud storage, and encrypted devices located in other countries. **In *Joined Cases C-339/20 and C-397/20 (CJEU, 2022),*** the Court ruled on the compatibility of national data retention laws with EU law, ensuring that traffic data could be shared across borders while respecting fundamental rights.

Effective coordination in investigation and prosecution is also vital. Courts and authorities must align timing, investigative methods, and legal standards to maintain the admissibility of evidence internationally.

5. Current Trends and Challenges in Judicial Cooperation

There are promising signs that judicial cooperation is advancing especially within the EU with strides also being taken within the AU:

I. Regional and Global Frameworks for Cooperation

For example; within the EU, the Budapest Convention provides a framework for cooperation among a wide array of relevant stakeholders. This framework allows for cooperation to the widest extent possible; application of urgent measures to preserve data; Use of efficient mutual legal assistance (MLA) mechanisms.[10]

The African Union's Malabo Convention sets standards for cybersecurity, personal data protection, and cooperation.

The United Nations Convention against Cybercrime was adopted by the General Assembly of the United Nations on 24 December 2024 in New York. The Convention is the first comprehensive global treaty on this matter, which provides States with a range of measures to be undertaken to prevent and combat cybercrime. It also aims to strengthen international cooperation in sharing electronic evidence for serious crimes. The Convention will open for signature on 25 October 2025 at a signing ceremony to be held in Hanoi, Viet Nam.

II. Practical tools for cooperation

[10] Chapter III of the Convention on Cybercrime (Budapest Convention)

Mutual Legal Assistance Treaties (MLATs) remain the backbone of cross-border evidence sharing. They allow states to request digital data, testimony, or investigative support from each other.

III. Transborder Communication channels

The integration of law enforcement networks with judicial cooperation frameworks represents a holistic response, where investigators and prosecutors work in tandem internationally.

IV. Judicial networks

Judicial networks such as the African Judicial Dialogue, the Ibero-American Judicial Summit, and the European Judicial Network foster communication and knowledge exchange are also very important tools for experience sharing and learning.

V. Capacity building

Capacity-building initiatives from organisations like INTERPOL, the African Union, and UNODC are equipping judges, prosecutors, and investigators with technical expertise.

In spite of the above, major challenges remain. These include:

a. Jurisdictional Issues

Cybercrime often involves actors, victims, and infrastructure located in multiple countries simultaneously, raising complex questions of jurisdiction. Determining where a crime was committed and which country has the authority to prosecute is challenging. In *Yahoo! Japan phishing scams (2014),* cybercriminals targeted users in multiple countries from servers located in the U.S. and Europe. Prosecutors faced difficulties deciding whether Japanese authorities or U.S. authorities had primary jurisdiction, highlighting the complications of overlapping jurisdictions.

b. Divergent legal definitions/applications

An act criminalized in one country may not be prosecutable in another. This divergence creates safe havens for offenders.

c. Legislative gaps/ Weaknesses in the judicial system

Unlike traditional crimes, cybercrime often does not require physical presence, making the adversarial litigation system poorly suited to such cases. In addition, even countries with comprehensive cybercrime laws enforcement challenges because laws cannot anticipate all evolving cyber threats.

d. Difficulties in evidence collection

Digital evidence is highly volatile and can be altered or deleted quickly, making timely collection critical. Traditional Mutual Legal Assistance processes are often too slow to preserve such evidence. Unequal technical capacities among jurisdictions risk creating safe havens for perpetrators. Some countries lack advanced forensic tools or trained personnel to investigate complex cybercrime, forcing reliance on foreign authorities.

6. Strengthening Cross-Border Judicial Cooperation

How then can we strengthen judicial cooperation in combating cybercrime? I offer a few suggestions here:

a. First, harmonisation of legal frameworks. For example, aligning definitions and procedures to reduce conflict in laws. Encouraging States to ratify Conventions that provide for cooperation.
b. Second, encouraging countries without cybercrime laws to adopt such legislation.
c. Third, creating specialized judicial institutions dealing with cybercrime.
d. Fourth, the adoption and ratification of robust International agreements.
e. Fifth, judicial cooperation through clarifying territorial jurisdiction vs. provider control to overcome obstacles in transborder acquisition of electronic evidence from cloud providers (Schwerha, 2010).
f. Lastly, expedited cooperation mechanisms We need fast-track judicial channels, allowing courts to validate urgent cross-border requests for digital evidence, etc

g. Safeguarding human rights in cybercrime cooperation. Finally, and importantly, surveillance or data transfer does not compromise individual freedoms. This is especially critical for societies emerging from conflict or democratic transitions, where trust in institutions is fragile.

Ultimately, while appreciating the challenges that cybercrime poses, it is of utmost importance that any framework dealing with this threat must remain grounded in the rule of law and respect for human rights.

I thank you very much for your kind attention.