# CND THEMATIC DISCUSSIONS SESSION 3

## "THE CRIMINAL MISUSE OF INFORMATION AND COMMUNICATION TECHNOLOGIES FOR ILLICIT AND DRUG-RELATED ACTIVITIES IS INCREASING"

**21 OCTOBER 2021**

**Time: 10:30 – 18:30 (Vienna time)**

**Intervention Statement**

**by Abel Basutu (PhD)**

**Senior Drug Control Programme Officer**
**African Union Commission**

Anecdotal evidence through member state reports to the African Union and also the continental drug surveillance network shows that criminals have targeted Africa using online communication technologies for organized crime including drug trafficking, human trafficking, small arms trafficking, illicit and counterfeit goods smuggling, illicit financial flows, money laundering, and online child sexual exploitation and abuse among others.

Organised crime networks are active in Africa and use platforms that include the Darknet, the Clearnet, Social Media and encrypted messaging applications.

Like other geographical locations, Africa has been vulnerable to organized crime which fuels corruption, infiltrates business and politics and hinders development. Firearms proliferation fuels civil wars and conflicts and hamper aspirations for a peaceful and secure continent espoused under the AU Agenda 2063 flagship project on **Silencing the Guns**.

Information Communication Technologies extend traditional drug trafficking into virtual domains, creating new communication channels and marketing platforms. This convenience of technology to drug trafficking and related organised crime has heightened the need for intelligence and forensic intervention and vigilance.

Africa is turning into a super highway for heroin trafficking via the Indian Ocean and we know much of it is aided by the abuse of ICTs. For example, online sales of drugs have been reported in South Africa and many other countries on the continent resulting in large shipments of heroin on the high seas of Eastern Africa, and that of cocaine off-shore in the Atlantic Ocean,

while on-shore shipments are made through harbours and airports across the continent.

Anecdotal evidence from the West African Epidemiology Network on Drug Use indicates increased anonymity of communications through encryption and anonymous ways to purchase and pay for the illicit substances.

Darknet websites are used for the sale of substandard, spurious, falsified and counterfeit medicinal products in West Africa, in addition to pharmaceuticals containing controlled substances diverted from licit supply channels.

Illegal sales of pharmaceuticals are facilitated by websites that disguise themselves as Internet pharmacies and supply controlled narcotic drugs and psychotropic substances without fulfilling the legal and administrative requirements established for traditional pharmacies. These websites mislead the public, particularly with the use of the term **“Internet pharmacy”.**

The growth in the sale of prescription drugs over the Internet is presenting drug safety regulators and law enforcement with a serious challenge.

There’s therefore an urgent need to safeguard electronic-health technologies and quality of online health information by taking appropriate measures to address illegal and harmful media content for drug-related activities through inter alia:

- Adequate legislative and regulatory provisions to respond timely to the illegal sale of internationally controlled substances through the internet (e.g. a Cyber Crime Bill)
- Legislation to regulate operations of "Internet Pharmacies"

- Monitoring supply channels of pharmaceuticals and controlled substances to prevent diversion.
- Strengthening Intra and Inter-agency collaboration for rapid exchange of data.

The African Union has been working with its member states, through its various continental frameworks and programmes, to strengthen capacities to counteract drug trafficking and related organised crime.

AFRIPOL was established as a specialized institution of the African Union for police cooperation against transnational organized crime. Easy and secure communication is critical in this regard. All the police agencies of the Member States have received basic equipment to facilitate easy and secure communication as well as sharing of data.

The AU Convention on Cyber Security and Personal Data Protection of 2014 (also known as the Malabo Convention) imposes obligations on Member States to establish legal policy and regulatory measures to promote cybersecurity governance as well as control cybercrime. Unfortunately, Member States are slow to ratify this Convention.

Our member states need to invest heavily in countering ICT related crimes through enhancing the capacity of law enforcement agencies to ably detect, prevent, investigate and prosecute criminal gangs involved in illicit drug trade in addition to establishing effective border control measures.

We reiterate the need to strengthen measures to address crime prevention and criminal justice reform, with emphasis on international cooperation on combating transnational organized crime.

We further urge member states to strengthen implementation of all the nine pillars of the AU Plan of Action on Drug Control and Crime Prevention (2019-2023) to counter the worsening situation concerning drug availability, use and its negative consequences.

Thank you.