COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT (CSTD)

Twenty-seventh session
Geneva, 15-19 April 2024

Submissions from entities in the United Nations system, international organizations and other stakeholders on their efforts in 2023 to implement the outcomes of the WSIS

Submission by

United Nations Office on Drugs and Crime

This submission was prepared as an input to the report of the UN Secretary-General on "Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels" (to the 27th session of the CSTD), in response to the request by the Economic and Social Council, in its resolution 2006/46, to the UN Secretary-General to inform the Commission on Science and Technology for Development on the implementation of the outcomes of the WSIS as part of his annual reporting to the Commission.

UNODC's contribution to

the SG report on progress made in 2023 on the implementation of the outcomes of the World Summit of the Information Society (WSIS)

Part One: An executive summary (half a page) of activities undertaken by all stakeholders, progress made, and any obstacles encountered.

During the reporting period, UNODC continued to provide secretariat services to the **Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes**, to facilitate the development of a new United Nations convention on cybercrime. At the same time, UNODC continued to provide tailored technical assistance to Member States to prevent and combat cyber-dependent and cyber-enabled crimes through capacity building and technical assistance.

The Office continued to address the increasing threat of online and ICT-facilitated **gender-based violence**, including **child sexual exploitation** and **abuse online**, through capacity-building and enhanced coordination among relevant actors, maximizing the synergies of UNODC thematic expertise and mandates on gender in the criminal justice system and cybercrime.

Moreover, the Office worked to provide criminal justice actors with practitioner-oriented guidance on **the application of new and advanced technologies** in the field of crime prevention and criminal justice **to enhance the rule of law** in accordance with the international human rights framework, while safeguarding against potential risks and unintended consequences.

Finally, as criminal networks and terrorist groups are increasingly relying on information technology to carry out their activities, UNODC has continued to adjust its programmes and technical support to Member States accordingly, including by introducing components on the **emergence and use of new technologies and payment methods** in its technical assistance activities.

Part Two: A brief (1–2 pages) analytical overview of trends and experiences in implementation at the national, regional and international levels and by all stakeholders, highlighting achievements and obstacles since WSIS and taking into account the follow-up and review of the 2030 Agenda for Sustainable Development. This could include information on the facilitation process of implementation, monitoring and cooperation among stakeholders.

<u>Strengthening ICT infrastructure in Africa</u>

Crime prevention in Southern Africa

UNODC continued to support Member States in Southern Africa to prevent and combat threats related to **trafficking in persons, gender-based violence and illicit drug use** by providing equipment ranging from computers and printers to biometric scanners and database equipment to strengthen ICT infrastructure in the **Democratic Republic of the Congo, Mozambique, Namibia, South Africa**, and **Zambia**.

Ensuring delivery in countries without an established UNODC presence, however, has required significant coordination with the Resident Coordinator's Office, and collaborative procurement via the UNDP office has emerged as a streamlined, cost-effective solution. It is imperative, however, to ensure the infrastructure's usability. As underscored by Namibian Carceral Services, while equipment may be available, ancillary requirements like Wi-Fi and training in data processing are essential for optimizing their utilization. Moving forward, it is crucial to address such nuances, ensuring that the ICT support is not just available but fully functional, and adapted to the unique needs of each beneficiary.

Access to health in prisons in Morocco

The value of ICT platforms can also be seen in UNODC's work to support the **modernization of health units in custodial settings**, where in **Morocco** for instance, the procurement of new technology and equipment has resulted in the update and/or improvement of the country's health information system in prisons.

Digitalization of criminal justice systems

UNODC's Global Review of Emerging Evidence on the Impact of COVID-19 on Criminal Justice System Responses to Gender-based Violence Against Women documented innovative programmes and measures undertaken by criminal justice institutions in various countries. It found that **e-justice mechanisms** have the potential to facilitate women's access to justice not only during lockdown or movement restrictions, but also in ordinary times, by addressing obstacles they usually face, such as corruption, high costs, delays, backlog of cases, as well as cultural and physical barriers to travelling outside their villages or communities.

UNODC's pilot research on the **use of technology in the criminal justice system** found that criminal justice practitioners cited cost effectiveness and improved system performance as key drivers for the use of technology in criminal justice processes. Other drivers include improving access to justice for victims, witnesses and accused persons, and ensuring enhanced access to legal information, and the increased transparency of criminal justice processes.

Respondents noted concerns regarding the application of certain technologies. Chief among these is the potential for criminogenic and discriminatory outcomes arising from the use of artificial intelligence for predictive purposes in both legal and law enforcement settings. The research identified that predictive technologies are afforded considerable weight by criminal justice actors in the absence of mechanisms for transparency, oversight or accountability regarding their operation. Further concerns related to the risk that a reliance on technology to create efficiencies (in clearing court backlogs, for example) may divert attention from addressing root causes of an over-burdened criminal justice system.

Introduction of ICT components in technical assistance for border management

In 2023, to strengthen the effectiveness of its trainings through realistic simulations, UNODC integrated **computer-based training modules with Virtual Reality** (VR) technology and distributed VR tools to frontline customs officers and law enforcement officials in **Southeast Asia**. UNODC also conducted preliminary training sessions for counterparts to familiarize them with VR technology. The use of virtual simulations for capacity building training proved successful, enabling the training sessions to bridge the complexities and safety challenges that often occur in the field.

Part Three: A brief description (1–2 pages) of:

(a) Innovative policies, programmes and projects which have been undertaken by all stakeholders to implement the outcomes. Where specific targets or strategies have been set, progress in achieving those targets and strategies should be reported.

In strengthening Internet governance:

- UNODC closely engaged with stakeholders, including relevant non-governmental organizations, civil society organizations, academic institutions and the private sector, so as to facilitate their participation as observers in the elaboration of a **new international convention in the area of cybercrime** by Member States, notably through assisting with the organization of five intersessional consultations of the Ad Hoc Committee and stakeholders, in line with General

Assembly resolution 75/282, in which stakeholders had the opportunity to present their views on key elements of the future convention, as well as to discuss those views with Member States[1].

- In June 2023, UNODC organized a comprehensive Expert Group Meeting on the **Removal of Child Sexual Abuse Material from the Internet**, bringing together governments, civil society organizations, development banks as well as the private sector to foster cooperation and public private partnerships to proactively remove and combat child sexual exploitation and abuse online. The event led to the adoption of the Call to Action Statement for Removing child sexual exploitation and abuse materials, which has been adopted by 73 Member States.

In ICT capacity building, including e-Learning:

Cybercrime

- UNODC provided support to 67 Member States in West Africa, Central Asia, Latin America and Southeast Asia and the Pacific, in increasing their knowledge of international best practices, increasing their specialized capabilities and improving standard operational procedures of the justice system to **attend cyber-enabled and cyber-dependent crimes**, with a special focus on cyber investigations, digital forensics, evidence handling cryptocurrencies, online child sexual abuse and exploitation and cybercrime prevention.
- UNODC developed an **e-learning course** on fundamentals of cybercrime and translated the cryptocurrency course into 8 languages. The **report "Darknet Threats Report to Southeast Asia"** was translated into three additional languages to increase awareness at policy and operational level. Cybercrime prevention materials for teachers and parents are available in English and Spanish, and also in a format accessible for people with impaired visibility and hearing.

Transnational organized crime

- UNODC has integrated digital technologies into capacity-building training targeting government officials and law enforcement in **Southeast Asia**, building their capacities in countering the **illicit trafficking of drugs and precursors** and **migrant smuggling by sea**. UNODC has developed and distributed 96 computer-based training modules tailored to strengthen the capacities of counterparts to address security challenges in the region. The modules have been translated from English into seven languages spoken in the region: Bahasa Indonesia, Burmese, Khmer, Lao, Malay, Thai and Vietnamese.
- To strengthen the capacity of counterparts in **Southeast Asia** on countering the increasing cases of **smuggling of migrants by sea**, UNODC designed a two-week training course that employs computer-based virtual simulation to replicate Crime Scene Investigation in smuggling vessels for law enforcement and maritime agencies. Through the computer-based virtual simulation, participants were able to train within realistic representations and real-life scenarios. Five trainings have been delivered in three countries in Southeast Asia, and modules were translated into Bahasa Indonesia, Malay, and Thai languages.
- UNODC supplied twenty laptops configured as servers and sixty VR goggles to the **Office of the Narcotics Control Board** (ONCB) of **Thailand** to facilitate the use of VR technology. The equipment was installed within the training facilities of ONCB and **border management** offices, with the objective of being available for the present and future generations of law enforcement officials, ensuring sustainability and avoiding its effectiveness being impacted by staff turnover.

Terrorism

- To respond to the growing threat posed by terrorist use of the Internet, UNODC delivered a training on **online investigative techniques** and handling **electronic evidence** with a view to strengthen capacity of national law enforcement and criminal justice practitioners in **Rwanda**. Additionally, UNODC supported the development of model forms to seek electronic evidence

[1] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

for national service providers. This assistance also included capacity-building activities for counter-terrorism officials on requesting **electronic evidence** in terrorism-related cases in **Pakistan**.

In using ICT to enhance international cooperation in criminal matters:

- UNODC's **Sharing Electronic Resources and Laws On Crime (SHERLOC) knowledge management portal** aims to facilitate the dissemination of information regarding the implementation of the United Nations Convention against Organized Crime (UNTOC), the Protocols thereto and the international legal framework against terrorism. In 2023, SHERLOC has grown to include over 3,480 case summaries of organized crime and terrorism prosecutions, more than 12,220 annotated extracts of legislative provisions, and over 240 national and regional strategies.
- ICT solutions have proven invaluable in advancing international judicial cooperation, as exemplified through UNODC tailored **mutual legal assistance (MLA) case management system**, which has been provided to the General Prosecutor Office in **Lebanon**. The system will allow the national authorities to keep track of MLA requests back to 2019 and will contribute to strengthening the exchange of information and international cooperation in criminal matters in the region.

In integrating ICT in education and youth engagement:

- UNODC implemented the **First Arab Youth Anti-Corruption Hackathon** (CODING4INTEGRITY) in partnership with the Administrative Control and Transparency Authority (ACTA) and Microsoft in **Qatar**. The primary objective was to actively involve emerging software developers from the Arab region in crafting ICT-driven solutions to address corruption-related issues. Initiatives such as this highlight the profound value of ICT dimensions in development, as well as the potential of south-south cooperation and innovation, and the value of locally or regionally owned solutions to the challenges.

On the role of ICT applications in e-governance:

- In order to support State parties' participation in the review mechanism through their appointed focal points and governmental experts to conduct country reviews in the context of the UNTOC Review Mechanism[2], UNODC continued the work on the development of the **REVMOD platform** and relevant tools (manuals and e-learning module) with the purpose of facilitating the use of the platform. In addition, UNODC strives to deliver regular REVMOD trainings in the six official languages, as well as in Portuguese. By 10 October 2023, 2,711 focal points and governmental experts from 150 countries had participated in the activities.

(b) Future actions or initiatives to be taken, regionally and/or internationally, and by all stakeholders, to improve the facilitation and ensure full implementation in each of the action lines and themes, especially with regard to overcoming those obstacles identified in Part Two above. You are encouraged to indicate any new commitments made to further implement the outcomes.

UNODC is currently preparing for a workshop to be held during the 15th Crime Congress, in 2026, on the topic of "***Turning the digital age into an opportunity: promoting the responsible use of technologies in crime prevention and criminal justice***", with the following objectives:

a) Consistent with the guidance in the Secretary-General's *Roadmap for Digital Cooperation*, to discuss practical strategies and partnerships to achieve digital inclusion, digital trust and

[2] https://www.unodc.org/unodc/en/organized-crime/intro/review-mechanism-untoc/home.html

security, digital human rights and digital cooperation in the field of crime prevention and criminal justice.

b) More specifically, to explore strategies to promote effective, coordinated and inclusive technology governance, including the development and implementation of rules among public and private sectors to prevent and counter the use of technologies for criminal purposes, to ensure that technology use aligns with international law, and to ensure that digital technologies and the Internet function as a sustainable global public good.

c) To discuss strategies for enhancing digital inclusion, based on the principle of leaving no one behind, and with particular attention to gender dimensions, intersectionality, and the rights and needs of specific groups (including women, children, the elderly, persons with disabilities, etc.) to enhance equal access to digital technologies, data, and knowledge (the digital commons) as a facet of crime prevention strategies and as means of enhancing equal access to justice for all.

d) To discuss how technologies can assist with the strengthening of data collection, analysis, and application in criminal justice systems, mindful also of data protection safeguards, and human rights considerations including privacy and other fundamental freedoms (movement, assembly, association, etc.).

e) To identify opportunities to further leverage technology to identify and combat cybercrime and the malicious use of technology (including new and emerging technologies).