COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT (CSTD)

Twenty-ninth session
Geneva, 20-24 April 2026

Submissions from entities in the United Nations system, international organizations and other stakeholders on their efforts in 2025 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 29th 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 2025 on the implementation of the outcomes of the World Summit of the Information Society (WSIS)

(Reporting period: 2025 and the last quarter of 2024)

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 strengthened the capacity of Member States to address both the challenges and opportunities posed by new technologies in countering terrorism. The Office also enhanced its engagement with legislators to help shape a robust international legal framework to prevent the misuse of artificial intelligence (AI).

Key activities included a series of high-level events on AI and the misuse of information and communications technologies (ICT), such as: the Vienna Symposium; the Aqaba Process meeting in London; the expert meeting in Geneva; and the regional workshop in Nairobi. UNODC also conducted missions to Riyadh and the Maldives focused on countering technology-facilitated terrorism and supported the Parliamentary Dialogue in Rome on countering AI misuse.

In addition, UNODC continued to assist Member States in signing, ratifying, and implementing the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes adopted by the General Assembly in 2024. Once fully implemented, this Convention is expected to reduce cybercrime risks faced by individuals, institutions, and countries, thereby promoting a safer and more resilient digital environment.

Overall, progress was made in fostering multi-stakeholder cooperation and enhancing regional capacities. Nevertheless, significant challenges remain, particularly the rapid adaptation of AI-driven tools and the use of encrypted platforms by terrorist actors, while legislative frameworks are uneven across regions and operational responses struggle to keep pace.

Part Two: A brief (1 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.

The increase in use and adaptation of Information and Communication Technologies, including artificial intelligence and digital wallet providers, by terrorist groups has become

an alarming trend and may provide these groups with powerful tools to incite violence and commit terrorist acts, as highlighted in the Eighth Review of the Global Counter-Terrorism Strategy (A/RES/77/298).

Discussions held across UNODC-supported international events in 2025 revealed several converging trends. The misuse of artificial intelligence (AI) has evolved beyond disinformation and propaganda to encompass operational planning, deepfake manipulation, and the exploitation of financial technologies. Terrorist groups increasingly weaponize AI to radicalize and recruit individuals, as well as to erode public trust. At the same time, AI presents significant opportunities for enhancing investigative tools and predictive analytics in counter-terrorism efforts.

Regional experiences demonstrate that while generative AI holds great potential for early threat detection and analysis, it also poses risks related to algorithmic bias, limited oversight, and potential human rights violations. These insights underscore how legal and parliamentary frameworks remain uneven across regions. While some Member States are advancing regulatory and governance mechanisms for AI, others continue to face legislative and enforcement gaps, creating potential safe havens for terrorist exploitation. Addressing these disparities requires more than technological innovation alone—it demands operational readiness built on trust, international cooperation, and strong public–private partnerships.

During the reporting period, notable achievements included strengthened cross-border cooperation, the mainstreaming of human rights considerations in counter-terrorism technology initiatives, and expanded multistakeholder engagement involving academia, civil society, and the private sector. However, significant obstacles persist, including legislative gaps, uneven digital literacy, limited cooperation with smaller online platforms, and ongoing challenges in safeguarding human rights within rapidly evolving technological environments.

Part Three: A brief description (half 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.

UNODC advanced several innovative initiatives including:

➢ Vienna Symposium (March 2025): Highlighted AI's dual role in countering terrorism and the need for ethical safeguards.
➢ Geneva Expert Meeting (May 2025): Emphasized human oversight in AI-assisted decisions.
➢ Nairobi's Regional Meeting in collaboration with CTED and UNOCT (August 2025): Strengthened capacity of Eastern Africa region against ICT misuse.
➢ Adoption of "Crescer em Paz" (Brazil, 2025): Brazil adopted a national strategy integrating ICT tools and child protection measures through systematic integration of

multi-stakeholder ICT governance, enhanced digital security for vulnerable populations, and rights-based ethical frameworks in digital child protection, establishing a replicable model for other countries developing similar strategies.

➢ UNODC Youth Peace Champions under the STRIVE Juvenile project, (Nigeria): The initiative protects children from crime and violence through a series of targeted interventions across the conflict-affected areas, including in building digital skills, strategic communication tools and community engagement techniques to counter violence and promote child-sensitive advocacy.

➢ UNODC & INTERPOL Neurotechnology Project: Explores the implications of neurotechnology for law enforcement and the criminal justice system and developing globally relevant, scientifically rigorous and human-rights based guidance for criminal justice officials to support the integration of the assistive and rights-supportive uses of neurotechnology.

➢ Coding4Integrity Asian Youth Anti-Corruption Hackathon (Hong Kong, China): Co-hosted the initiative aiming to engage young people and promote the use of technology in fostering a culture of innovation in the fight against corruption. UNODC supported the participants in developing their solution prototypes of technological solutions for corruption-related issues affecting their communities.

(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 will continue to promote responsible integration of AI and ICTs in countering terrorism, including developing international model laws on AI use and digital evidence. Future actions include: strengthening regional cooperation mechanisms in Eastern Africa; expanding capacity-building programmes to enhance digital literacy for law enforcement, parliamentarians, and communities; and deepening public-private partnerships with technology companies. Support to Member States will focus on refining legislative frameworks in-line with human rights obligations, ensuring that technological responses to terrorism are ethical, effective, and sustainable.