UNODC

United Nations Office on Drugs and Crime

LASALLECUNMUN 2026

"Strategic use of digital intelligence to dismantle transnational crime."

BACKGROUND GUIDE

With great honor, I welcome you to the United Nations Office on Drugs and Crime (UNODC) committee. I am honored to serve you, and I look forward with great interest to our dialogues being productive and our work collaborative during this model. My name is Fernando Espino Olmedo, and I have the great privilege of being your President this year. Alongside me, you will also find the support of our Moderator, Danna Paola Rodriguez Corral, and Brissa Elena Suastegui Rivero, as your Conference Officer.

I am 17 years old, and I am in my third semester of high school at Universidad La Salle Cancún, specifically in the area of Administration and Business Development. I haven't decided on a career path yet, but I am interested in anything related to finance, numbers, or law. Outside of my academic life, I love spending time with loved ones, listening to music, running, and playing tennis. However, there is one activity in particular that I love: building Legos. I also love the Batman movie trilogy.

This is my second time participating in the model; the first time I was a delegate, but this time, I decided to be President because I wanted to make a change in my life and in the lives of those around me, aiming to change the world through positive actions. "Success is not measured by what you achieve, but by the obstacles you overcome." With this phrase, we invite you to actively participate and achieve a great model.

I trust that this committee will be a space for learning, respect, and constructive debate, where each delegate can contribute their ideas and strengthen their oratory, analysis, and negotiation skills. My wish is for each of you to feel motivated to give your best, remembering that, beyond everything, the most valuable thing is the experience we build together.

My best wishes to you,

Fernando Espino Olmedo

United Nations Office on Drugs and Crime (UNODC)

unodc@prepa.lasallecancun.edu.mx

COMMITTEE DESCRIPTION

Established in 1997, the United Nations Office on Drugs and Crime (UNODC) works to make the world safer from drugs, crime, terrorism, and corruption. We operate in 150 countries, building networks of cooperation across borders and providing reliable data and analysis. UNODC also trains judges, police officers, and border officials, as well as healthcare and social workers, to make communities safer and more resilient.

Topic: "Strategic use of digital intelligence to dismantle transnational crimes."

INTRODUCTION

Transnational crime—ranging from human trafficking and drug smuggling to cybercrime and terrorism—presents an increasingly complex challenge. In our hyper-connected world, advances in communication and transportation have allowed criminal networks to operate more quickly and stealthily, exploiting legal loopholes and jurisdictional borders. Traditional law enforcement methods are no longer sufficient to confront these ever-evolving threats.

Consequently, Artificial Intelligence (AI) has emerged as a powerful tool, enabling the instantaneous analysis of data to identify patterns and even anticipate suspicious movements before they occur. This study critically reviews how technologies such as Machine Learning (ML), predictive analytics, and biometric systems can help detect, prevent, and combat transnational crimes. While these technologies can transform investigations, the report also addresses sensitive issues: potential algorithmic bias, data privacy, and the ethical necessity of international cooperation.

Ultimately, the goal is to ensure that AI is used responsibly within the framework of international security, promoting clear legislation and robust cooperation between nations to ensure that technological progress does not compromise human rights.

Digital technologies are increasingly being exploited by human traffickers and migrant smugglers to expand their reach. However, the criminal justice sector has also benefited from these innovations. Every online transaction leaves a digital trail; by using advanced data collection and analysis, investigators can better track illicit activities and secure vital digital evidence.

The UNODC supports these efforts by providing criminal justice professionals with Open Source Intelligence (OSINT) techniques—tools essential for dismantling entire transnational networks and identifying individual perpetrators.

HISTORICAL BACKGROUND

The United Nations Office on Drugs and Crime (UNODC) was established in 1997 when the UN merged its departments dedicated to justice and drug control. In 2002, it officially adopted its current name. Since then, its primary mission has been to support member states in addressing transnational issues such as drug trafficking, corruption, terrorism, and money laundering.

Beyond its administrative role, UNODC has become a vital pillar for governments striving to maintain security and justice. In recent years, the advancement of Information and Communication Technologies (ICTs) has fundamentally altered the landscape of transnational crime. We are no longer merely discussing organizations operating on physical streets or across borders; today, many operate via computers and smartphones. Criminal groups now utilize cryptocurrencies, encrypted messaging, offshore accounts, and dark web platforms to move funds, coordinate with collaborators, and recruit victims—all while minimizing their digital footprint.

This "digitalization" of crime has significantly complicated investigations. Securing evidence and locating perpetrators is increasingly difficult, requiring unprecedented international cooperation as a single crime can originate on one continent and conclude on another. Consequently, States face a new paradigm: crime that requires neither a physical presence nor a conventional weapon, but merely a stable internet connection and a false identity.

While criminal organizations operate with the agility of a modern corporation, many legal frameworks remain outdated. A significant technological gap exists; while some nations possess advanced digital forensic tools, others struggle to track even basic digital communications. This disparity allows criminals to remain several steps ahead of government jurisdictions.

Recognizing that no State can tackle this alone, the UNODC launched its Strategy 2021–2025. This was not merely a document, but a proactive effort to bridge the gap between law enforcement and digital reality. The strategy focuses on fundamental capacity building: investigating digital environments, handling electronic evidence, and fostering cross-border cooperation. Furthermore, the organization promotes international norms on emerging issues like Artificial Intelligence (AI) and data analytics for tracking illicit networks.

Initiatives such as CRIMJUST were established to connect States along trafficking routes, enabling them to share digital intelligence and conduct joint operations. The UN maintains that technology is neutral; its impact depends on whether it is used to facilitate crime or to dismantle it. Therefore, UNODC continues to champion the Convention against Transnational Organized Crime while spearheading debates for a new international treaty on cybercrime.

On the International Day of Police Cooperation, Secretary-General António Guterres acknowledged the immense potential of AI and ICTs for crime prevention and prosecution.

However, he emphasized that their use must be responsible, transparent, and always uphold human rights. In Southeast Asia, UNODC has highlighted how criminal groups exploit illegal online casinos, cryptocurrency laundering, and deepfakes. Similarly, in jurisdictions like Pakistan,

UNODC has trained counter-terrorism officers in Open Source Intelligence (OSINT), social media analysis, and digital literacy.

Ultimately, the challenge is not only technological but political. If nations do not modernize their laws and strengthen their collective will, they will continue to fall behind the evolving tactics of global crime.

CURRENT SITUATION

The current landscape of transnational crime is expanding rapidly as criminal networks exploit digital technologies to operate at high speed and on a massive scale, often bypassing existing national and international institutional structures. The intentional tactical application of digital intelligence has become both a primary tool for managing this threat and a critical priority for global institutions, placing the United Nations Office on Drugs and Crime (UNODC) and its partners at a decisive juncture.

Criminal organizations now utilize encrypted communications, cryptocurrencies, "darknet" marketplaces, and AI-driven fraud schemes to engage in human trafficking, migrant smuggling, illicit financial flows, and cyber-enabled fraud. Consequently, States must act decisively to build capacities in digital forensics, lawful data usage, and cross-border harmonization to ensure that intelligence can effectively stop these activities.

Several key developments have shaped recent years:

1. Convergence of Technologies: Criminal business models—especially in drug and human trafficking—are now embedded in cyber-enabled ecosystems. Digital platforms allow for recruitment, financing, and execution with lower visibility and greater speed than traditional smuggling routes.
2. Increased Coordination: International bodies have ramped up coordinated actions. The UNODC's *"Digest of Cyber Organized Crime"* argues that ICTs have had a transformational impact on organized crime, necessitating intelligence-led responses.
3. The Rise of the Scam Industry: Flagship reports highlight the growth of the cyber-fraud industry, particularly in Southeast Asia. This sector generates billions through forced labor, "pig-butchering" investment scams, deepfakes, and cryptocurrency flows. The UNODC notes that these illicit markets are currently outpacing the response capacities of most States.

The UNODC maintains that digital intelligence must not only be reactive but also strategic, focusing on the upstream collection, analysis, and fusion of data. This requires:

- Legal Frameworks: Facilitating timely mutual legal assistance and the sharing of electronic evidence.
- Asset Intelligence: Tracking blockchain transaction flows and device forensics to map network nodes.

- Means Intelligence: Implementing machine learning for anomaly detection and AI-based analytics.

Crucially, these operational tools must be guided by robust safeguards for human rights, data protection, and the rule of law.

Failure to advance in this field would have dire consequences. Operationally, criminal networks will migrate to less regulated territories under the protection of powerful patrons, adopting resilient technologies faster than authorities. Legally, a lack of global consensus on digital intelligence would foster impunity, as prosecutions would fail without substantial evidential leverage. In short, the inability to modernize will allow criminal infrastructures to automate and expand with irreversible global spillover.

COUNTRY BOX

Bolivarian Republic of Venezuela

Canada

Commonwealth of Australia

Federal Republic of Germany

Federal Republic of Nigeria

Federative Republic of Brazil

French Republic

Islamic Republic of Iran

Islamic Republic of Pakistan

Kingdom of Saudi Arabia

Kingdom of the Netherlands

People's Republic of China

Republic of Cuba

Republic of Singapore

Republic of South Africa

Republic of Türkiye

Russian Federation

State of Japan

United Kingdom of Great Britain and Northern Ireland

United Mexican States

United States of America

GUIDE QUESTIONS

I. What is your country's official position regarding the strategic integration of digital intelligence into national security frameworks to combat transnational organized crime?

II. What legislative measures, specialized units, or technological initiatives has your nation implemented to investigate and prevent crimes facilitated by Artificial Intelligence and other emerging technologies?

III. How has the expansion of cyber-enabled transnational networks specifically impacted your country’s socio-economic stability, national security, or critical infrastructure?

IV. What concrete proposals does your delegation put forward to enhance cross-border cooperation, facilitate the exchange of electronic evidence, and harmonize international legal standards for the use of digital intelligence?

V. What specific legal safeguards and transparency mechanisms does your country propose to ensure that the use of digital intelligence tools remains consistent with international human rights law and the right to privacy?

BIBLIOGRAPHY

I. Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

II. Global Initiative Against Transnational Organized Crime. (2023). *Global Organized Crime Index 2023*. https://globalinitiative.net/analysis/ocindex-2023/

III. OECD. (2023). *Artificial Intelligence*. https://www.oecd.org/en/topics/artificial-intelligence.html

IV. UNODC. (n.d.). *Oficina de las Naciones Unidas contra la Droga y el Delito*. https://www.unodc.org/

V. UNODC. (n.d.). *OSINT - UN Toolkit on Synthetic Drugs*. https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/OSINT.html

VI. UNODC. (n.d.). *Using the Power of Technology to Help Victims of Human Trafficking*. https://www.unodc.org/unodc/frontpage/2022/July/using-the-power-of-technology-to-help-victims-of-human-trafficking.html

VII. UNODC. (2024, October). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

VIII. UNODC. (2024). *UNODC Facilitates Discussions on the Ethical Use of Artificial Intelligence and Advanced Technologies to Prevent and Counter Terrorist Exploitation of Online Spaces in South-East Asia*. https://www.unodc.org/unodc/en/terrorism/latest-news/2024-unodc-facilitates-discussions-on-the-ethical-use-of-artificial-intelligence-and-advanced-technologies.html