



Background Guide

United Nations Office on Drugs and Crime (UNODC)



Letter From Chairs

Dear Delegates,

As the chairs of the UNODC council, Nirupama Menon and Aahana Koul, on behalf of the United Nations Office on Drugs and Crime (UNODC), send you our best wishes as you get ready to take part in the upcoming NMMUN '25. We are so happy to have you speak for your nation and participate in conversations about important current-world scenarios.

During the conference, the UNODC council will focus on two significant topics over the course of two days:

Day 1: Combating Organised Crime in Climate Displaced Regions.

The discussions will revolve around the intersection between organized crime and climate change, addressing the challenges faced by migrants and the means through which organized crime groups accelerate the issue.

Day 2: Cybercrime and the Dark Web: International Counter-measures

The discussions will revolve around the global threat posed by cybercrime, their effect on trust in digital systems and the undermining of privacy and security. We will also debate upon the importance of cooperative frameworks in strengthening cybersecurity.

We urge you to thoroughly examine these issues, become familiar with the position of your nation, and arrive prepared with well-reasoned arguments backed up by pertinent data and analysis.

Delegates, remember—everyone started out nervous at some point. Don't let the pressure overwhelm you. Focus on expressing your ideas with clarity and passion rather than perfection. Confidence grows with every speech, so take a deep breath and speak from conviction—you've got this. Our goal as chairs is to facilitate this process and assist our delegates as honestly as possible. Kindly do not hesitate to contact us in the event that you need any help before, during, or even after the

conference. We hope to meet and have a fantastic conference with all of you, and we wish you the best of luck.

Best Regards,

Nirupama Menon
Grade 10
New Millennium School

Aahana Koul
Grade 11
New Millennium School

About UNODC

UNODC is a global leader in addressing the problem of illicit drug use and transnational crime and is mandated to assist Member States in their struggle against illicit drugs, crime, and terrorism.

UNODC was established in 1997 because of the merger of the United Nations Centre for International Crime Prevention and the United Nations International Drug Control Programme.

It was established by the Secretary-General of the United Nations to enable the Organization to focus and enhance its capacity to address the interrelated issues of drug control, crime, and international terrorism in all its forms.

The International Narcotics Control Board is a permanent and independent body, consisting of 13 members who are elected for a five-year term by the Economic and Social Council based on their competence and serve in their personal capacity.

UNODC Mandate and Structure

The mandates of UNODC include the areas related to transnational organized crime, criminal justice, countering corruption, drug control, and terrorism. This allows the Office to provide comprehensive solutions to the interrelated challenges Member States face. Strong institutions that have integrity and accountability will provide effective responses and access to justice. Moreover, effective institutions are also key to promoting a balanced response to drugs.

The Office helps ensure that efforts to address crime, corruption, terrorism, and drugs are coordinated across national boundaries, facilitating our shared responsibility in addressing these challenges.

Of relevance to UNODC mandates are human rights related to the areas of justice, security, and health.

The prevention and reduction of all forms of violence and abuse should be at the heart of any agenda that fully recognizes the centrality of human security, both as a human rights imperative and as being integral to development.

The Commission on Narcotic Drugs, composed of 53 Member States elected by the Economic and Social Council for a four year term, is the central policy-making body regarding drug related matters, including the monitoring of the global trends of illicit drug trafficking and abuse.

This functional commission of the Economic and Social Council adopts and recommends for adoption by the Council or to the General Assembly through the Council, resolutions on new concerted measures or agreed policies to better address the drug phenomenon. It decides whether new substances should be included in one of the schedules of the conventions and if changes or deletions in the schedules are required.

The Board monitors the implementation of the conventions and, where appropriate, makes recommendations to States. It also administers the statistical control of drugs since data supplied by Governments and assesses world requirements of licit drugs with a view to the adaptation of production to those requirements. It gathers information on illicit trafficking and submits an annual report on developments in the world situation to the Commission on Narcotic Drugs and to the Economic and Social Council.

Combating Organised Crime in Climate Displaced Regions

Introduction

As climate change speeds up, causing more frequent and severe disasters, it forces people to leave their homes, creating a new and complicated security problem. When social systems break down, people lose their jobs, and government control weakens in areas affected by climate change, this allows organized crime groups to grow. These groups take advantage of vulnerable displaced people by engaging in human trafficking, smuggling migrants, and extorting money. They also benefit from illegal activities, like stealing natural resources, which worsen environmental damage.

Climate change-related events, such as droughts, floods, and hurricanes, have led to an increase in migration flows. The main causes of migration that often overlap with the effects of climate change, such as lack of education, job opportunities and stable housing further highlights the link between climate change, human trafficking, and migrant smuggling. Research has revealed that climate change exacerbates inequality, increasing people's vulnerability to trafficking

To tackle this interconnection between climate displacement and organized crime, we need a comprehensive approach that goes beyond regular security methods. addressing both the impacts of climate change and the rise of crime through international cooperation and support for affected communities.

Definition of Key Terms

- **Climate-displaced regions** - Areas where people have been forced to leave their homes — temporarily or permanently — because of the impacts of climate change or climate-related disasters.
- **Organized Crime**- A structured group of individuals acting together over time to commit serious offenses for financial or material gain.
- **Human Trafficking**- The harboring or transporting of persons by means of coercion, fraud, or deception for exploitation.
- **Smuggling of Migrants**- The illegal facilitation of border crossings for profit. (In climate displacement contexts, smugglers often exploit people escaping environmental disasters or unlivable conditions.)
- **Internally Displaced Persons (IDPs)**- People who have been forced to flee their homes but remain within their own country's borders
- **Environmental Crime**- Illegal acts that directly harm the environment. These crimes are often linked to organized criminal networks that exploit natural resources and displaced populations.

Past UN action:

- **The Global Action against Trafficking in Persons and the Smuggling of Migrants – Asia and the Middle East (GLO.ACT-Asia and the Middle East)**- It is a four-year joint initiative by the European Union (EU) and the United Nations Office on Drugs and Crime (UNODC) being implemented in partnership with the International Organization for Migration (IOM).
- **Protocol Against the Smuggling of Migrants by Land, Sea and Air (2004)**: Adopted by the UN General Assembly, this protocol established an internationally agreed-upon definition for the smuggling of migrants and aims to bring an end to it.
- **Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (2003)**: This protocol criminalized human trafficking and required states to work together to protect victims and prosecute traffickers. UN Secretary-General António Guterres has explicitly acknowledged that climate change exacerbates the vulnerabilities that allow trafficking to flourish
- **UNODC- Crimes that Affect the Environment (CAE)**: The United Nations Office on Drugs and Crime has explicitly acknowledged that many environmental crimes (illegal logging, mining, wildlife trafficking, etc.) are linked to organized criminal networks, which then undermine climate resilience, harm livelihoods and exacerbate displacement.
- There is increasing work on the rights of internally displaced persons (IDPs) when displacement is driven or worsened by criminal violence. For example, a thematic report and side event in mid-2025 co-organized by the **GI-TOC, UNODC, and the Special Rapporteur on the human rights of IDPs** discussed organized criminal activity as a driver of displacement.

Timeline

- 1) 1990 : The First UN Recognition of Climate Displacement
 - a) The IPCC First Assessment Report suggests that climate change could be the cause of large scale human displacement. Thus, the UN formally links climate change with forced movement of people.

- 2) 2004 : Indian Ocean Tsunami and Rise in Exploitation Risks
 - a) The tsunami is the cause of displacing millions across South and South-East Asia.
 - b) Due to the tsunami, UNODC reports spikes in trafficking and child exploitation especially in the regions that were mainly affected.

- 3) 2013 : Warsaw International Mechanism for Loss of Damage (WIM)
 - a) It was formally introduced at COP19. The UNFCCC framework explicitly includes human mobility in its mandate.
 - b) This establishes a common policy globally for climate displacement.

- 4) 2015 : Paris Agreement (COP21)
 - a) Article 8 of the Paris Agreement mentions displacement which led to the formation of the Task Force on Displacement (TFD) under WIM.

- 5) 2023 : UNGA and COP28 Turning Points
 - a) According to IDMC's Grid 2024 Report, 26 million people were displaced by climate related disasters.
 - b) UNHCR's 2024 Report suggests that climate displacement is increasingly being exploited by criminal organizations.

Relevant Information

The effects of climate change are recognized more and more as a reason for both sudden and slow onset human displacements - floods or hurricanes and then droughts or desertification. The report, IDMC Global Report on Internal Displacement 2024, claims that more than 26 million individuals were displaced due to climate catastrophe. This also happens to be the highest number that has been recorded in a single year, 2023. Displaced individuals more often than not migrate to city centers or the border of other countries. This has the tendency to put the individuals at risk of various crimes such as exploitation, trafficking, forced labor, and other crimes related to syndications.

The organized crime scene has several ways to prey on these victimized groups. As the victimized groups are placed in their rightful position in society by displacement, the criminal networks then thrive in trafficking and smuggling because those victims do not enjoy legal protection, documentation, or even social support. Displaced populations are also liable to be pushed into forced labor in a shadow economy or illegal means of livelihood-giving, such as illegal logging, mining, or fishing, in areas suffering from environmental degradation.

The UNODC has categorized climate-induced displacement as an "emerging risk multiplier" for organized crime. The UNODC reports build the nexus between disasters and forced migrations and higher incidence of trafficking and cross-border smuggling. While the UNTOC framework, along with its Protocols on trafficking and migrant smuggling of the UNODC, provide the legal framework under which these crimes could be dealt with in a disaster context, its GLOTIP reports track changing patterns of exploitation.

Several UN mechanisms work on the side of climate displacement, criminality being particularly targeted by a few. The WIM and the Task Force on Displacement formulate policy recommendations to assist States in managing climate-induced mobility. The PDD operationalizes practical measures, such as temporary protection and planned relocation, to protect displaced people. However, while the GCM (2018) does recognize climate change as a driver of migration, it also urges States to cooperate in preventing trafficking and exploitation.

In addition, protection gaps feed into the problem. The persons displaced by climate sometimes are not recognized as refugees under international law, hence remaining without protection and vulnerable to abuse by criminal groups. Additionally, the discrepancy in data on displacement and crime hinders coordinated intervention, with IDMC, UNHCR, and national estimates often diverging.

Multi-agency cooperation will have to address the issues at hand. Mapping of risks, strengthening legal enforcement, and other measures should be undertaken in cooperation with UNODC, UNHCR, IOM, and national governments.

Guiding Questions for Debate

Should the UN recognize a new legal category of “climate refugees”, and what would be the implications for state responsibility?

To what extent should climate-displaced populations be treated as a security risk versus a human rights concern?

What are the most effective strategies to combat trafficking, smuggling, and exploitation in climate-displaced communities?

Possible Solutions

- Making climate-displacement / mobility a regular factor in threat assessments related to organized crime (i.e. understanding where and how displacement creates opportunities for exploitation by criminal networks).
- Strengthening protection frameworks for displaced persons (IDPs/refugees) specifically against criminal exploitation, trafficking, smuggling etc. ensuring human rights are central.
- Greater legal innovation: possibly new treaties or protocol(s) to explicitly address crimes arising from climate change effects (resource grabs, land grabbing, environmental degradation).

Cybercrime and the Dark Web: International Countermeasures

Introduction

In today's rapidly evolving digital age, cybercrime has emerged as one of the most compelling global security concerns. With growing usage of the internet and technological innovation, crime groups have new avenues for conducting illicit operations ranging from money laundering, thefts, and hacks on data to large-scale ransomware assaults and human trafficking, weaponry, and narcotics trade. Among the most important drivers for this boom is the dark web—a hidden and considerably unpoliced aspect of the internet that provides anonymity to users. While the dark web was originally designed to preserve privacy and free speech, it has also emerged as an incubator of transnational organized crime, cyber terrorism, and illegal commerce.

Cybercrime, a criminal activity carried out by computers and the internet, has become one of the most growing global security challenges. The dark web is the part of the internet where users can access web content anonymously through special web browsers like The Onion Router (Tor). This anonymity enables illegal trade in weapons, drugs, stolen data etc. While encryption and crypto currencies transform readable data to unreadable data to safeguard privacy, they also make it easier for criminals to elude detection.

The United Nations Office on Drugs and Crime (UNODC) can play a crucial part in solving these problems since cybercrime does not respect borders and calls for a multilateral approach. There is a need to combat the misuse of the dark web through law enforcement collaboration, international cooperation in terms of law, cyber capacity development, as well as human rights protection in cyberspace. This problem thus presents a challenge to the delegates in balancing the promise of digital technology and its urgent requirement for curbing its misuse, so that cyberspace remains a safe, secure, and capable environment for all.

Definition of Key Terms

- **Cybercrime:** It refers to socially dangerous acts committed using computer equipment against information processed and used in cyberspace.
- **Dark Web:** It is the World Wide Web content that exists on darknets (overlay networks) that use the internet, but require specific software, configurations, or authorization to access.
- **Anonymity Networks:** Systems such as Tor that hide user identity and location, enabling access to the dark web.
- **Cyber terrorism:** It is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.
- **Crypto currency:** It is a digital currency designed to work through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.
- **Ransomware:** Malicious software that locks data until a ransom is paid.
- **Budapest Convention (2001):** The first international treaty that addressed cybercrime.
- **Phishing:** It is a form of social engineering and a scam where attackers deceive people into revealing sensitive information or installing malware such as viruses, worms, adware, or ransomware.

- **Digital Forensics:** It is the process of collecting and analyzing digital evidence in a way that maintains its integrity and admissibility in court.

Past UN Action

- **The United Nations Office on Drugs and Crime (UNODC)** leads the effort with its Cybercrime Programme. It provides technical help, builds capacity, and offers policy advice to Member States, especially those in the Global South.
- **The United Nations General Assembly** is also working on a new convention on cybercrime. Negotiations are ongoing to find a balance between state sovereignty, privacy, and global security interests.
- In addition, international policing bodies have strengthened their cybercrime divisions. **INTERPOL's** Cybercrime Directorate helps with cross-border intelligence-sharing and joint operations.
- **Europol's European Cybercrime Centre (EC3)** offers operational support to EU Member States.
- **The International Telecommunication Union (ITU)** has started the Global Cybersecurity Agenda (GCA) to promote international cooperation and capacity-building.
- **Regional organizations like the African Union and Organization of American States (OAS)** have also developed cybercrime strategies to assist their Member States.

Timeline

2001 – Council of Europe’s Convention on Cybercrime (Budapest Convention)

- The first international treaty to combat computer crime and establish cooperation among states.
- Serves as a legal model for UN member states and international law enforcement cooperation.

2008 – Rise of the Dark Web

- Dark web marketplaces begin facilitating illegal transactions, including drugs, weapons, and stolen data.
- Cybercriminal networks exploit anonymity tools like Tor and crypto currencies, complicating law enforcement efforts.

2013 – Global Attention on Data Breaches & Cybercrime

- High-profile events like the Edward Snowden revelations and large-scale hacking incidents push the UN to discuss privacy, cyber security, and cross-border cybercrime.
- UNODC and INTERPOL start highlighting cybercrime as a major transnational organized crime threat.

2015 – UNODC Cybercrime Program Expansion

- UNODC develops technical assistance programs, focusing on capacity-building, cyber law enforcement, and digital evidence collection.

- Member states encouraged to integrate cybercrime policies into national legislation.

2018 – Dark Web & Crypto currency Regulation Debate

- Rapid growth of dark web markets using crypto currencies raises questions about regulation, monitoring, and anti-money laundering measures.
- UN bodies begin promoting international cooperation and intelligence sharing to tackle dark web criminal activity.

2020 – COVID-19 Pandemic & Cybercrime Surge

- Lockdowns and increased online activity lead to spikes in phishing, ransom ware, and online scams.
- UNODC reports emphasize the need for coordinated international frameworks to combat cybercrime and dark web exploitation.

2023 – UNGA Resolutions on Cyber security & Dark Web

- UNGA calls for strengthened cybercrime prevention, international cooperation, and capacity-building in digital investigations.
- UNODC emphasizes the link between cybercrime and transnational organized crime, including dark web trafficking and illicit trade.

Relevant Information

Cybercrime, with far-reaching effects on households, businesses, and states, is fast becoming one of the most pressing challenges of the digital era. It encompasses acts of all kinds, ranging from hacking to identity theft, from ransom ware to phishing, from financial fraud to digital platforms being employed for organized crime. According to UNODC, cybercrime is now a major ingredient of transnational organized crime that exploits the internet's attribute of anonymity and global reach.

Another major enabling factor for cybercrime is the dark web-a clandestine internet space requiring special software, such as Tor, to access. The dark web, initially meant to afford anonymity and privacy, is now a major venue for illegal activities- drug sales, arms deals, counterfeit documents, stolen data, and child sexual exploitation material. It abets crime syndicates in coordinating smuggling, trafficking, and money laundering. The rise of crypto currencies has only furthered this, allowing transactions outside of traditional banking systems and rendering interdiction that much more difficult.

The cybercrime spectrum is enormous. Global losses due to cybercrime run into trillions of dollars in a year, with ransom ware attacks shutting down critical infrastructure, healthcare systems, and financial institutions. The COVID-19 pandemic further accelerated cybercrime activities since the transition into online work and commerce created fresh vulnerabilities. Many states, especially developing ones, are incapable of technically investigating or prosecuting these crimes effectively, thereby making them most vulnerable.

In response, international frameworks have come into being. The most renowned international treaty still has to be the Council of Europe's Budapest Convention on Cybercrime (2001), which essentially promotes harmonization of laws and cooperation across national borders. The UNODC Cybercrime Program offers technical support and capacity-building assistance, as well as legislative support, to member states. In 2021, the General Assembly created an open-ended Ad Hoc Committee to draft a new Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes, on the occasion of the present-wide shift towards a UN-level legal framework on cybercrime.

These efforts aside, considerable controversies do persist. A few states want to enhance global regulation and surveillance to curb dark web activities, whereas others lay utmost importance on safeguarding privacy, human rights, and freedom of expression. Moreover, discord exists between developed and developing states:

while developed economies have developed cyber capabilities, developing states argue they should get more help in terms of technology transfer and capacity-building to effectively combat cybercrime.

Guiding Questions for Debate

How can international law balance the need for cross-border cooperation with the protection of state sovereignty in cyberspace?

Should states focus on shutting down dark web marketplaces or on strengthening monitoring and law enforcement capacity?

How can UNODC ensure that cybercrime enforcement measures do not violate privacy, data protection, or freedom of expression?

Possible Solutions

- **Improving Digital Literacy:** Educate individuals and companies by developing cybersecurity awareness campaigns that talk about media risks and prevention methods.
- **Monitoring The Dark Web:** Encourage all states to develop special dark web investigation units with proper ethics and standards.
- **Strengthening Legal Frameworks:** Promoting The Budapest Convention and encouraging all states to adopt cybercrime legislation.
- **Promoting Human Rights and Data Protection:** Ensuring all the international countermeasures respect human rights, privacy and freedom of expression.
- **Enhancing Cross-Border Cooperation:** Establish an international coordination under UNODC to facilitate sharing of information between law enforcements.

Bibliography

- <https://www.unodc.org/unodc/en/human-trafficking/glo-act2/Countries/rising-concerns-of-climate--crime-and-exploitation-addressed-at-commission-on-crime-prevention-and-criminal-justice-side-event.html>
- <https://www.unodc.org/unodc/en/human-trafficking/glo-act/index.html>
- https://convention2.allacademic.com/one/apsa/apsa18/online_program_direct_link/view_paper/1374494/
- [Sustainable Dev Knowledge Platform+4unis.unvienna.org+4UNODC+4](https://www.univie.ac.at/development/knowledgeplatform/)
- <https://unis.unvienna.org/unis/en/pressrels/2023/uniscp1163.html>
- <https://globalinitiative.net/announcements/protection-of-internally-displaced-persons-in-the-context-of-organized-criminal-activity/>

- <https://www.unodc.org/unodc/index.html>

- <https://www.interpol.int/Crimes/Cybercrime>

- <https://www.coe.int/cybercrime>