Letter by The Executive Board

Dear Delegates,

Welcome to BBIMUN 2026- UNODC. We are beyond excited to meet you and are eager to welcome you at two days of productive and stimulating debating. For us, Model United Nations have become integrated into our lifestyle, we view it as educational as much as it's empowering to have the ability to construct opinions on global issues through the eyes of several different countries. We hope that as soon as you log into the committee session, you learn something new and that hopefully by the end of the conference you have grown in one way or another; whether it's your ability to overcome your fear of public speaking or your ability to lead large groups of people.

If this is your first Model United Nations Conference, then don't worry too much and feel free to approach any of us at any point in the conference if you need any form of support. Please do not hesitate to reach out to any of us for any concerns you have. We cannot wait to meet all of you! A MUN conference does not end when the committee session is over, every conference broadens your mind and urges you to think differently and analytically. This document should not by any means bind your research to its limits.

As the Executive Board, we are committed to ensuring that this year's Model United Nations is a resounding success. We have been working tirelessly to create an enriching and engaging experience for all participants. Our goal is to foster a spirit of diplomacy, cooperation, and intellectual discourse among all delegates.

We believe that this year's conference will be particularly significant as we continue to grapple with global issues such as climate change, economic inequality, and social justice. We recognize the importance of providing a platform for young leaders to exchange ideas and propose innovative solutions to these pressing challenges.

To this end, we have assembled a talented and diverse team of organizers and committee chairs who are eager to facilitate dynamic and thought-provoking debates as we approach the conference. We encourage all delegates to prepare thoroughly and engage fully with the topics at hand. We hope that this experience will inspire you to continue pursuing your passion for international affairs and making a positive impact in the world.

This guide is just an introduction to the agenda and serves as the starting point for your research. Feel free to revert to the executive board for any queries or for any form of assistance that you may require. It has been long overdue that all of us unite against the vices of our time to move ahead towards the utopian world we have promised to the future generations. It is with this hope that we wish you luck for the conference. The background guide is not made to spoon feed you so that we are able to test your analytical bent of mind and the committee can come to a common ground and not consider the background guide as the bible.

Regards,

Siddhant Magon- Director General
Parishi Gupta - Deputy Director General
Tanish Mittal - Substantive Director

Introduction to the Committee

The United Nations Office on Drugs and Crime (UNODC) is the United Nations entity responsible for supporting Member States in addressing illicit drugs, transnational organized crime, corruption, terrorism and related criminal-justice challenges. Established in 1997 through the merger of the United Nations Drug Control Programme and the Centre for International Crime Prevention, UNODC is headquartered in Vienna and works through a global network of field and regional offices. Its work combines policy support, research and data, technical assistance, capacity-building and assistance in implementing international legal instruments.

UNODC also supports the work of the Commission on Narcotic Drugs (CND) and the Commission on Crime Prevention and Criminal Justice (CCPCJ), the two principal UN policy bodies dealing with drugs and crime respectively. In addition, UNODC served as the secretariat for the Ad Hoc Committee that negotiated the United Nations Convention against Cybercrime. This makes the Office particularly relevant to an agenda that sits at the intersection of drugs, organized crime, cybercrime and international cooperation.

Why UNODC is directly relevant to this agenda

The present agenda is broader than cyber security alone. Digital platforms can connect buyers and sellers in illicit drug markets, criminal groups can use online services to recruit or exploit victims, and cyber-enabled offences can generate proceeds that move across borders through digital payment systems. UNODC approaches these problems from a criminal-justice and international-cooperation perspective: strengthening laws, investigative capacity, digital-forensics capabilities, cross-border cooperation and the ability of prosecutors and courts to use electronic evidence. Its Global Programme on Cybercrime specifically covers cyber-dependent and cyber-enabled crime, online child sexual exploitation and abuse, digital evidence and illicit use of virtual assets.

What UNODC can contribute

For delegates, an important distinction is between setting norms and implementing them. UNODC does not replace national police, prosecutors or courts, and it does not independently enforce criminal law across borders. Its role is to help Member States develop compatible legal frameworks, strengthen institutions and professional capacity, improve international cooperation, and generate evidence and technical guidance that can support implementation. In the context of this agenda, this includes assistance on cybercrime legislation, electronic evidence, investigations, prosecution, digital forensics, prevention and cooperation between competent authorities.

Why this matters for committee debate

Delegates should therefore approach the agenda with two questions in mind. First, what international rules or mechanisms are still missing, unclear or difficult to use? Second, how can those rules be implemented across States with very different legal systems, resources and technological

capabilities? A strong outcome will need to bridge both problems. The debate is not only about creating new offences; it is also about evidence, jurisdiction, safeguards, capacity-building and practical cooperation.

Introduction to the Agenda

Cybercrime is often discussed as if it were a narrow technology problem. It is not. A phishing operation can become fraud; a compromised account can become a channel for trafficking; a social-media contact can become the first step in child exploitation; and a digital payment trail can connect an online offence to an organised criminal network operating across several jurisdictions. **The practical difficulty is that criminal law is still organised mainly around territory, while digital evidence, platforms, money flows and offenders are not.**

The 2024 United Nations Convention against Cybercrime is therefore an important starting point, but not the end of the discussion. As of 20 September 2026, the Convention has been signed by 82 participants and has 3 parties; it has not yet entered into force. The Budapest Convention, meanwhile, remains a mature operational framework with 82 parties. The gap between adopting a treaty and making it useful in a real investigation is precisely where much of the committee's work should sit.

What is changing?

The digital environment has altered the scale and speed at which familiar crimes can be committed. Malware, fraud, trafficking, drug sales and sexual exploitation did not begin with the internet, but digital systems can reduce geographic barriers, multiply victims, automate parts of an operation and leave evidence in a service provider's system rather than at the location where the crime occurred. The same infrastructure can also produce legitimate benefits, which is why the central legal problem is not simply "more enforcement", but enforcement that is targeted, lawful and workable across borders.

The UN Cybercrime Convention expressly connects cybercrime with serious offences such as money-laundering, trafficking in persons, drug trafficking, firearms trafficking and other transnational crime. It also provides for cooperation on electronic evidence and technical assistance, while requiring implementation consistent with international human rights law and respecting State sovereignty.

The three parts of the agenda

• **Cybercrime:** conduct directed at computer systems or data, as well as selected cyber-enabled conduct such as computer-related fraud.

• **Digital drug trafficking:** the use of social media, encrypted communications, darknet markets and digital payment systems to advertise, negotiate, finance or facilitate illicit drug transactions.

UNODC's 2026 findings estimate darknet drug-related sales at around US$2.5 billion in 2025, while noting that much retail activity now occurs on social media.

• **Online exploitation:** child sexual exploitation and abuse, grooming, financial sexual extortion, non-consensual dissemination of intimate images and the misuse of generative AI to create or manipulate abusive material. WeProtect's 2025 assessment identifies encrypted spaces, AI-generated abuse material and financial sexual extortion as important parts of the changing threat landscape.

Why the Issue Has Become Harder

The location of the offence is no longer obvious

A victim may be in one country, the offender in another, the platform incorporated in a third and the relevant data stored in several more. Traditional mutual legal assistance can become slow relative to how quickly digital evidence can disappear.

Criminal markets are becoming less centralised

Darknet markets remain relevant, but UNODC's recent research points to a shift toward social-media retail and more wholesale activity on darknet markets. Criminal groups can migrate between platforms rather than relying on one permanent marketplace.

Technology changes faster than statutes

Generative AI, synthetic media, encrypted services and new financial technologies can create conduct that sits awkwardly inside older criminal-law categories. Europol's 2026 IOCTA similarly highlights encryption, proxies and AI as forces changing the cybercrime landscape.

More evidence can also mean more intrusive investigation

The ability to access subscriber data, traffic data, content and cloud-stored material can help solve serious crimes, but it raises questions about proportionality, privacy, legal remedies and oversight. The UN human-rights assessment specifically raised concerns about the breadth of electronic-evidence provisions and the need for clear safeguards.

Capacity is uneven

A treaty can establish common rules, but a State still needs investigators, prosecutors, judges, digital-forensics capability, secure channels and trained personnel. The UN treaty expressly makes technical assistance and capacity-building a core purpose, with particular attention to developing countries.

Past Trends and Major Turning Points

Period	Turning point	Why it matters
2001	**Budapest Convention**	The Council of Europe Convention became the first major international treaty focused on cybercrime, combining criminalisation, procedural powers and international cooperation. It later developed a broad global membership beyond Europe.
2000s–2010s	**Digitalisation of organised crime**	Criminal groups increasingly adopted online communications, digital fraud, encrypted services and electronic payments. The internet stopped being merely a communications layer and became part of the business model.
2010s	**Darknet markets and platform migration**	Online drug supply expanded through both darknet marketplaces and clearer web/social channels. UNODC research has documented how internet and social-media growth changed drug distribution and reduced the number of intermediaries in some supply chains.
2015–2020	**Ransomware and cyber-enabled extortion**	Ransomware demonstrated how criminal groups could combine technical compromise, anonymous payment methods and transnational infrastructure. This pushed cybercrime toward the centre of international law-enforcement cooperation.
2020–2022	**Pandemic-era acceleration**	Greater dependence on digital services expanded the pool of potential victims and increased reliance on remote communications, online commerce and digital systems. Online exploitation also adapted to more time spent in digital spaces.
2019–2024	**UN treaty negotiations**	The General Assembly established the Ad Hoc Committee in 2019. After negotiations beginning in 2022, Member States adopted the Convention against Cybercrime in December 2024.
2025	**Signing stage**	The UN Convention opened for signature in Hanoi in October 2025. It is legally significant, but signature is not the same as ratification and the treaty has not yet entered into force.
2026	**Implementation and adaptation**	The policy debate has moved from negotiating the basic text to questions of ratification, domestic implementation, e-evidence procedures, AI-related exploitation and how regional systems fit together. The Council of Europe's 2026 work, including the Second Additional Protocol and AI-related child-exploitation guidance, illustrates this implementation phase.

Existing International Legal Architecture

The agenda does not begin with a blank sheet of paper. Delegates should understand how the new UN Convention sits alongside older instruments rather than treating it as a replacement for everything that existed before.

Instrument	Relevance to the agenda
UN Convention against Cybercrime (2024)	Global criminal-justice treaty adopted 24 Dec 2024. Covers core cyber offences, selected online exploitation offences, money laundering, international cooperation, electronic evidence, victim measures, technical assistance and capacity building. Not yet in force as of 20 Sep 2026.
Budapest Convention on Cybercrime (2001)	Operational framework covering criminalisation, procedural tools and international cooperation. The Council of Europe currently lists 82 parties. Its 24/7 network is designed to allow rapid preservation and cooperation concerning electronic data.]
Second Additional Protocol to the Budapest Convention (2022)	Adds enhanced tools for cross-border e-evidence cooperation, including direct cooperation with service providers and emergency cooperation mechanisms, subject to safeguards.
UN Convention against Transnational Organized Crime (UNTOC) (2000)	Broader organised-crime framework. It remains relevant where cyber-enabled conduct is carried out by organised criminal groups, and complements the cyber-specific instruments.
1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances	Core global drug-control treaty. Digital channels do not replace the underlying drug-control regime; they change how trafficking can be marketed, coordinated, financed and investigated.
Lanzarote Convention (2007)	Council of Europe framework focused on protecting children against sexual exploitation and sexual abuse. Its relevance has grown with online grooming, abusive material and AI-generated or altered content. In June 2026, the Cybercrime Convention Committee and Lanzarote Committee issued a joint statement on AI-generated or altered child sexual abuse material.
EU e-evidence framework	EU Regulation 2023/1543 and Directive 2023/1544 establish European Production and Preservation Orders and rules for designated establishments/legal representatives. The framework became applicable in stages during 2026.

Positions of Major Powers and Regional Blocs

The positions below are intended as a starting map, not a claim that any delegation will support every element described. Countries revise positions, make reservations and bargain issue-by-issue. Delegates should therefore distinguish a State's formal treaty position from broader policy statements.

State / bloc	Broadly documented position	Likely negotiation themes
United States	No signature is recorded in the UN Treaty Collection as of 20 September 2026. During the negotiations, the United States argued for a tightly focused, rights-respecting treaty, meaningful criminalisation, due process, privacy and civil-liberties safeguards, and continued use of the Budapest Convention. The U.S. warned against overly broad definitions that could be used to restrict legitimate conduct or expression.	Scope; human-rights safeguards; due process; interoperability with existing tools.
United Kingdom	Signed the UN Convention on 25 October 2025. The UK describes the treaty as complementing the Budapest Convention and has stressed human-rights safeguards, online fraud, child sexual abuse, non-consensual intimate-image dissemination and	Rights safeguards; practical law-enforcement cooperation; child protection; online fraud.

	cooperation with governments, industry and civil society.	
France	Signed the Convention on 25 October 2025. France describes the UN Convention as a useful addition to the Budapest framework, with an emphasis on maintaining a balance between investigative powers and procedural/human-rights safeguards. It has also said it will remain vigilant against misuse of the framework.	Procedural safeguards; European legal standards; international cooperation.
China	Signed the Convention on 25 October 2025. China has long advocated a UN-led cybercrime convention and emphasised a comprehensive approach, international cooperation, national practices and the needs of developing countries.	Universality; comprehensive coverage; sovereignty and national practice; capacity building.
Russian Federation	Signed the Convention on 25 October 2025 and has presented itself as the initiator of the UN treaty process. Russian materials and statements emphasise a legally binding multilateral framework, international cooperation and practical systems for electronic evidence.	UN-centred framework; international legal cooperation; electronic evidence; sovereignty.
European Union	The EU signed the Convention as a regional economic integration organisation. EU statements support the new treaty as a complement to existing instruments and stress fundamental-rights safeguards, effective cooperation and child protection. The EU's separate e-evidence framework also shows its focus on faster cross-border access to electronic evidence with procedural safeguards.	Fundamental rights; e-evidence; interoperability; child protection; strong procedural safeguards.
African Union	The AU's Malabo Convention provides a regional baseline on cybersecurity, electronic transactions and personal-data protection, and entered into force in 2023. In the UN cybercrime debate, African States have repeatedly emphasised practical international cooperation and capacity building, particularly where domestic criminal-justice and forensic capacity is limited.	Capacity building; regional legal harmonisation; data protection; implementation support.
ASEAN / East Asia Summit	ASEAN has developed regional cybercrime and transnational-crime cooperation, with emphasis on timely information sharing, capacity development and law-enforcement cooperation. A 2025 East Asia Summit statement also linked cybercrime, online scams and illicit drugs, and welcomed implementation of the UN Cybercrime Convention alongside regional mechanisms.	Regional cooperation; online scams; cybercrime; illicit drugs; practical coordination.
G7	The 2026 G7 Interior and Security Ministers' communiqué highlights ransomware, fraud, cyberscams and cryptocurrency theft, and supports international collaboration and the Global Fraud Summit. G7 statements have also encouraged use of the Budapest Convention and UNTOC.	Ransomware; fraud; crypto; critical infrastructure; law-enforcement cooperation.

India	India's 2021 submission argued for a comprehensive UN convention covering cybercrime broadly, drawing on existing instruments without duplication, with inclusive negotiations, practical solutions, capacity building and multistakeholder participation. Its position should be read alongside India's subsequent participation in the completed negotiations and the 2025 signing process.	Comprehensive coverage; inclusivity; capacity building; multistakeholder participation.

Key Issues

What exactly should the international framework criminalise?

The new Convention criminalises core conduct such as illegal access, interception, data and system interference, misuse of devices, computer-related forgery/fraud, online child sexual abuse material, grooming, non-consensual dissemination of intimate images and laundering of proceeds. The harder question is how far an international instrument should go beyond these offences, including in relation to cyber-enabled trafficking and emerging technologies.

How should cross-border electronic evidence work?

The practical problem is often not the absence of evidence but the inability to lawfully obtain it quickly. Delegates should examine preservation, production orders, emergency procedures, service-provider requests, mutual legal assistance, 24/7 networks and rules for authentication and admissibility. The Second Additional Protocol and the EU e-evidence system provide concrete models to compare.

Where should human-rights safeguards sit?

Questions include judicial authorisation, necessity, proportionality, purpose limitation, notice, appeal or review, privacy, protection of privileged material and remedies when a request is abusive. OHCHR's 2024 assessment specifically questioned provisions that allow electronic-evidence cooperation beyond core cybercrime and urged stronger safeguards.

Encryption and lawful access

End-to-end encryption can protect journalists, businesses and ordinary users while also limiting the ability of investigators to access certain evidence. There is no simple legal formula that resolves this tension. Delegates should distinguish targeted, judicially supervised access from proposals that weaken the security architecture for all users.

Online exploitation of children and adults

The agenda should not reduce "online exploitation" to illegal images. Grooming, sextortion, livestreamed abuse, financial exploitation, AI-generated material and non-consensual intimate-image dissemination raise different evidentiary and victim-protection questions. WeProtect's 2025 assessment points to AI and encrypted spaces as fast-moving areas of concern.

Digital drug trafficking and platform migration

UNODC's 2026 findings suggest a mixed market: darknet activity remains resilient, while social media has become important for retail sales. This raises questions about how evidence is obtained

from platforms, how payments are traced, how proceeds are frozen and how international drug-control rules interact with cybercrime rules.

Virtual assets and financial tracing

Cyber-enabled crime increasingly leaves a digital financial trail. The committee can explore common standards for identifying proceeds, freezing assets, handling virtual assets and cooperating with financial-intelligence and law-enforcement bodies without creating unworkable burdens.

Platform responsibility and public-private cooperation

Much of the relevant evidence is held by private companies. Delegates therefore face a design question: what should governments require, what should companies be expected to do voluntarily, and what safeguards should apply when private platforms respond to criminal requests?

Capacity building and implementation

A treaty that only a few highly resourced jurisdictions can implement will leave gaps elsewhere. Possible areas include training, digital forensics, model legislation, prosecutor and judicial capacity, secure channels, regional centres of excellence and financial support for implementation. The UN Convention expressly places capacity building near the centre of the framework.

How should the system evolve?

The UN General Assembly decided that the Ad Hoc Committee would continue work toward a supplementary protocol addressing additional criminal offences. Delegates should consider how the framework can be updated without requiring a completely new treaty every time technology changes.

Questions Delegates Should Carry Into Committee

- Which offences require harmonised criminalisation internationally, and which should remain primarily within domestic law?
- What should be the minimum legal standard before a State requests subscriber data, traffic data or content data from another jurisdiction?
- How can urgent evidence be preserved quickly without creating a parallel system that bypasses judicial or treaty safeguards?
- Should service providers ever be allowed or required to respond directly to foreign law-enforcement requests? Under what conditions?
- How should the treaty distinguish serious cybercrime from conduct that is politically controversial, embarrassing or merely unlawful under one State's domestic law?
- How should AI-generated or AI-altered abusive material be addressed while preserving legitimate research and lawful expression?
- What international measures can realistically disrupt digital drug markets when sellers can migrate between platforms?
- What support should be available to developing countries before they are expected to meet detailed investigative and evidentiary obligations?

- How should proceeds recovered from cyber-enabled crimes be traced, frozen and returned across multiple jurisdictions?
- What role should INTERPOL, UNODC, regional organisations, national cybercrime units, prosecutors, courts, financial-intelligence units and technology companies each play?

Possible Areas of Convergence

Delegates should not assume that a negotiating room will divide cleanly into “pro-enforcement” and “pro-privacy” camps. In practice, many delegations support both stronger investigation and stronger safeguards. The more productive debate is often about how to make those objectives operational at the same time.

- Common minimum offences combined with explicit legality and intent requirements.
- Faster preservation of digital evidence, followed by formal disclosure through recognised legal procedures.
- 24/7 points of contact and standardised request formats to reduce administrative delay.
- Judicial or independent oversight for intrusive evidence-gathering measures.
- Clear rules for emergency situations involving imminent risk to life or safety.
- Capacity-building programmes tied to measurable needs rather than broad statements of support.
- Formal channels for cooperation with service providers that include transparency and safeguards.
- Victim-centred provisions covering reporting, content removal where lawful, compensation, recovery and protection from repeated trauma.
- Periodic review of the framework so that technological change can be addressed without weakening core rights protections.

Research Links to Consider

[1] United Nations Treaty Collection: UN Convention against Cybercrime

[2] Budapest Convention: parties, structure and 24/7 network.

[3] UN General Assembly Resolution 79/243 and annexed Convention text.

[4] World Drug Report 2026: darknet sales and online drug-market findings.

[5] Global Threat Assessment 2025.

[6] IOCTA 2026: The evolving threat landscape.

[7] Human Rights Assessment of the Draft United Nations Cybercrime Convention.

[8] Use of the Dark Web and Social Media for Drug Supply

[9] Report of the UN Ad Hoc Committee on Cybercrime.

[10] Second Additional Protocol to the Budapest Convention.

[11] Technology-facilitated child sexual abuse: progress in investigations and training..

[12] 24/7 Network under the Budapest Convention

[13] E-evidence. European Commission..

[14] U.S. International Cyberspace & Digital Policy Strategy.

[15] UN Cybercrime Treaty Negotiations

[16] UK national statement on signing the UN Convention against Cybercrime.

[17] 2025 East Asia Summit Foreign Ministers' statement. ASEAN / EAS

[18] G7 2024 Foreign Ministers' Statement on global challenges

[19] India: views on scope, objectives and structure of a UN cybercrime convention