GDGSMUN

PAX ET RENOVATIO

INTERPOL

Letter from the EXECUTIVE BOARD

To,
The Honourable Members of INTERPOL
Subject: Message from the Executive Board to the Members of INTERPOL

Sir/Ma'am,
We hope this document finds you in excellent health.
To facilitate an engaging, easy-to-understand simulation of INTERPOL, the committee will not strictly adhere to the organisation's actual Rules of Procedure. Instead, the committee will blend the best practices of unorthodox committees across various MUN circuits with debating norms commonly followed at Model United Nations conferences and Youth Parliaments.

As this is the inaugural edition of GDGSMUN, we are delighted to welcome you to what promises to be an intellectually stimulating and enriching conference. The committee aims to provide delegates with a practical understanding of INTERPOL's functioning while exploring the complexities of the agenda, "Enhancing Cross-Border Investigations Against Criminal Networks Operating Through Encrypted Platforms."

Although this is an unorthodox committee, we are committed to ensuring that the proceedings remain accessible and engaging for both experienced delegates and first-time participants. The Executive Board will always be open to constructive suggestions that enhance participation and facilitate meaningful discussion throughout the committee sessions.

By the end of the two days of committee, we hope each delegate will have developed a deeper understanding of INTERPOL's mandate, operational mechanisms, and the challenges international law enforcement faces in combating technologically advanced transnational crime. We encourage you to approach the committee with curiosity, diplomacy, and an open mind, and we look forward to witnessing thoughtful debate and innovative solutions.

We wish you all the very best for your preparation and look forward to meeting you at GDGSMUN.

Best Regards,
Executive Board

Key definitions and KEYWORDS

1. INTERPOL

The International Criminal Police Organisation, commonly known as INTERPOL, is the world's largest international police organisation. Founded in 1923, its primary role is to facilitate the cooperation of law enforcement agencies across national borders to combat transnational crime. It helps law enforcement agencies worldwide exchange information and intelligence, track criminals, and coordinate efforts to tackle various forms of international crime. INTERPOL's primary mission is to ensure a safer world by facilitating cooperation between police forces across countries, providing a secure international network for the exchange of criminal information, and supporting police in tackling crimes such as terrorism, drug trafficking, human trafficking, cybercrime, and organised crime.

2. ENCRYPTION

Encryption is the process of converting readable information into an unreadable format so that only someone with the correct decryption key can access it. It is widely used to protect messages, files, financial transactions, and other sensitive information from unauthorised access. Today, encryption is an essential part of digital communication, helping ensure privacy, cybersecurity, and the secure exchange of information.

3. END TO END ENCRYPTION

End-to-End Encryption (E2EE) is a method of securing communication in which only the sender and the intended recipient can read the contents of a message. This means that even the service provider cannot access the communication while it is being transmitted. While E2EE has significantly improved user privacy and data security, it has also made it more challenging for law enforcement agencies to obtain digital evidence during criminal investigations.

4. TRANSNATIONAL CRIMINAL NETWORK

A transnational criminal network is an organised group that carries out criminal activities across two or more countries. These networks may include criminal cartels, which control illegal markets such as drug trafficking, and criminal syndicates, which are involved in crimes including human trafficking, cybercrime, financial fraud, money laundering, and arms smuggling. By operating across borders and using modern communication technologies, these groups can expand their operations while complicating investigations for law enforcement agencies. .

5. CRYPTOCURRENCY

Cryptocurrency is a form of digital currency that uses cryptography to secure transactions and operates without a central bank or financial institution. It allows individuals and businesses to transfer funds quickly across borders and has become an important part of the digital economy. However, its relative anonymity has also made it attractive for activities such as money laundering, ransomware payments, terrorist financing, and other forms of organised crime.

6. MUTUAL LEGAL ASSISTANCE TREATY (MLAT)

A Mutual Legal Assistance Treaty (MLAT) is an agreement between two or more countries that enables them to assist one another in criminal investigations and legal proceedings. Through these agreements, countries can exchange evidence, obtain electronic data, identify suspects, trace criminal assets, and execute other lawful investigative requests. MLATs are an important mechanism for strengthening international cooperation against transnational crime.

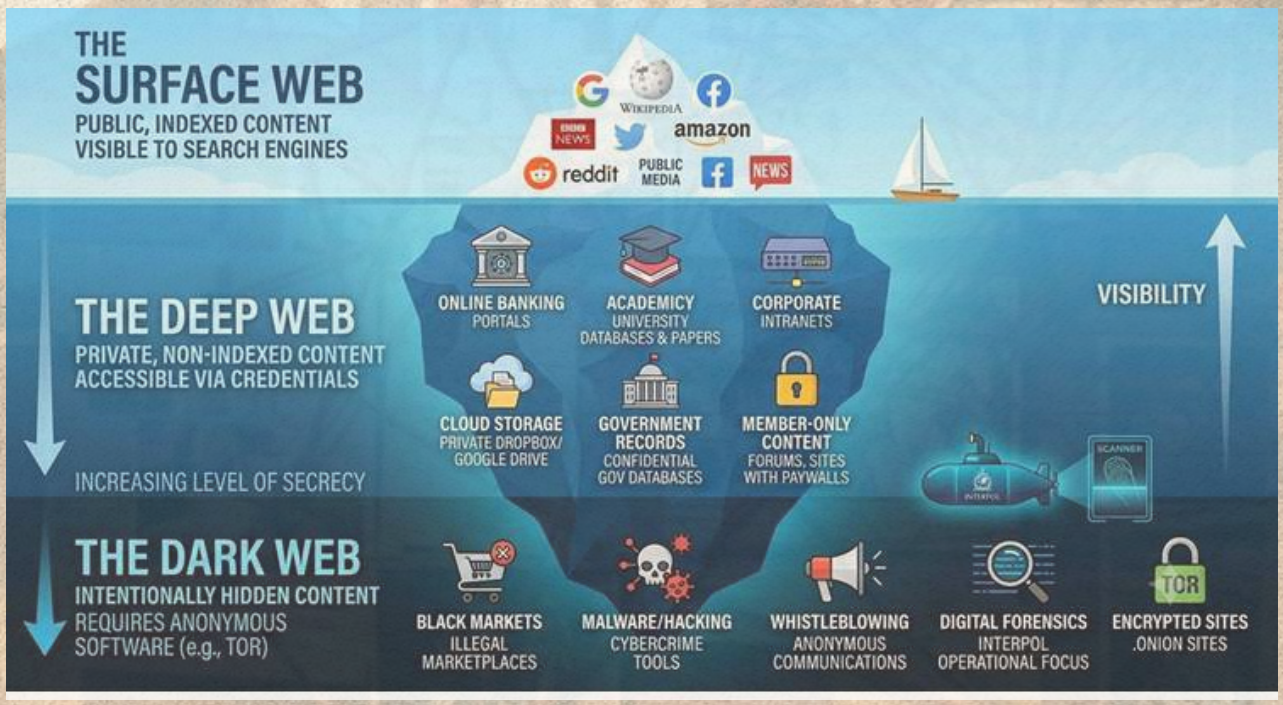
7. BACKDOOR POLICY

A Backdoor Policy refers to legislative or regulatory proposals that require technology companies to provide law enforcement agencies with lawful access to encrypted communications. Such proposals are generally justified on the grounds of national security and criminal investigations. Supporters argue that lawful access is essential for combating terrorism, organised crime, and child exploitation, while critics believe that creating backdoors could weaken encryption and expose users to cybersecurity risks. The issue remains one of the most debated topics in balancing digital privacy with public safety.

8. DEEP WEB AND DARK WEB

The Deep Web refers to all parts of the internet that are not indexed by conventional search engines such as Google or Bing. It includes password-protected websites, online banking portals, private databases, academic journals, cloud storage, and other content that requires authentication to access. The Deep Web is entirely legal and constitutes the majority of internet content. Law enforcement agencies, including INTERPOL, regularly use secure and restricted digital networks to exchange sensitive information without exposing it to the public internet.

The Dark Web is a small, intentionally hidden section of the Deep Web that can only be accessed using specialised software such as Tor (The Onion Router) or I2P (Invisible Internet Project). These networks conceal users' identities by routing internet traffic through multiple servers that encrypt it. While the Dark Web has legitimate uses related to privacy and freedom of expression, it is also exploited for illicit activities such as drug trafficking, illegal arms sales, stolen data markets, ransomware operations, and other forms of transnational organised crime.



9. GOING DARK PROBLEM

The Going Dark Problem refers to the growing gap between law enforcement agencies' legal authority to access digital communications under judicial authorisation and their technical ability to do so due to the widespread use of strong encryption technologies. As end-to-end encryption and device-level encryption become standard features, investigators may be unable to obtain critical evidence even with lawful authorisation.

This challenge is commonly divided into two areas:

- Data in Motion: Information being transmitted over the internet may be lawfully intercepted, but end-to-end encryption prevents investigators from reading its contents.

- Data at Rest: Information stored on encrypted devices, such as smartphones or computers, remains inaccessible without the user's passcode, as manufacturers generally do not possess the decryption keys.

10. ENCRYPTION IN SOCIAL MEDIA NETWORKS

Modern social media and messaging platforms primarily use two types of encryption:

- Transport Layer Security (TLS): TLS protects data as it travels between a user's device and a platform's servers. Once the data reaches the server, it can be decrypted and processed by the service provider.

- End-to-End Encryption (E2EE): E2EE ensures that only the sender and the intended recipient can read the contents of a message. Neither the service provider nor third parties can access the communication while it is in transit.

Based on their encryption models, communication platforms can generally be grouped into three categories:

- Conventional Social Networks: Platforms such as Instagram, TikTok, and X primarily rely on TLS and do not provide end-to-end encryption for most communications. Messages stored on their servers may be accessed for moderation, security, or lawful compliance.
- Dedicated Encrypted Messaging Platforms: Services such as WhatsApp and Signal use end-to-end encryption by default for messages, voice calls, and shared media, ensuring that communications remain private between users.

- Hybrid Platforms: Some platforms, such as Telegram, provide end-to-end encryption only through optional features like Secret Chats, while others offer E2EE only for selected conversations or specific types of communication.

II. ONION ROUTING

Onion Routing is a technique for providing anonymous communication over the internet by encrypting data in multiple layers before transmitting it through a series of intermediary servers, known as relays. Each relay removes only one layer of encryption, revealing the next destination without knowing the complete communication path. As a result, no single relay can identify both the sender and the final recipient of the communication.

Networks such as Tor (The Onion Router) typically use a three-hop circuit consisting of an Entry (Guard) Node, a Middle Relay, and an Exit Node. Separate encryption keys are established with each relay, ensuring the user's identity and the destination remain protected throughout the communication. While onion routing is widely used to safeguard privacy and freedom of expression, it is also exploited by criminal networks to conceal their online activities and evade law enforcement investigations.

Mandate and Functions of THE INTERPOL

The first and foremost mandate of INTERPOL is to coordinate cross-border efforts to prevent and combat various forms of international crime, including terrorism, drug trafficking, human trafficking, arms smuggling, cybercrime, financial crime, and other forms of transnational organised crime. It also provides a secure channel for the police forces of member countries to exchange criminal intelligence, digital evidence, and other sensitive information through its global communication network, I-24/7. Furthermore, INTERPOL provides technical expertise, digital forensic support, and specialised training to national law enforcement agencies, particularly in investigations involving cybercrime, encrypted communications, financial crime, and money laundering.

INTERPOL also develops and promotes international standards for law enforcement cooperation, information sharing, and criminal investigations. It bridges the gap between law enforcement agencies of different countries, ensuring effective cooperation in cross-border investigations, especially those involving encrypted communication platforms and digitally enabled criminal networks. As technology continues to evolve, INTERPOL has strengthened its efforts to assist member states in addressing cybercrime through operational support, intelligence sharing, cyber-capability development, and international cooperation. It also plays a significant role in combating transnational organised crime, including drug trafficking, arms smuggling, human trafficking, money laundering, ransomware, and other cyber-enabled criminal activities.

IINTERPOL provides a secure global communications system that enables member countries to exchange real-time criminal intelligence, including information on fugitives, missing persons, stolen property, digital evidence, and ongoing criminal investigations. It issues Notices to alert member countries about wanted persons, criminal threats, and persons of interest, with the Red Notice being the most widely recognised.

STRUCTURE OF INTERPOL

1. GENERAL SECRETARIAT

The General Secretariat, based in Lyon, France, serves as the administrative and operational centre of INTERPOL. It manages day-to-day operations, criminal intelligence analysis, and coordination among member countries. The General Secretariat also provides technical support, digital forensic expertise, and operational assistance to member countries in investigations involving cybercrime, encrypted communications, and other forms of transnational organised crime.

2. EXECUTIVE COMMITTEE

The Executive Committee oversees the work of INTERPOL's General Secretariat. It consists of 13 members elected by the General Assembly and is responsible for guiding the organisation's priorities, policies, and strategic direction. The Committee ensures that INTERPOL's activities remain consistent with its constitutional mandate while responding to emerging global security challenges

3. GENERAL ASSEMBLY

The General Assembly is the supreme decision-making body of INTERPOL. It consists of representatives from all member countries and meets annually. The General Assembly reviews and adopts policies, approves the organisation's budget, elects members of the Executive Committee, and determines INTERPOL's strategic priorities in addressing evolving forms of international crime.

4. PRESIDENT AND SECRETARY GENERAL

The President of INTERPOL serves as the ceremonial head of the organisation and chairs meetings of the General Assembly and Executive Committee. The Secretary General is responsible for the executive management of INTERPOL and oversees the General Secretariat's work, including international operations, intelligence coordination, and cooperation among member countries.

5. NATIONAL CENTRAL BUREAUS (NCBS)

Every INTERPOL member country maintains a National Central Bureau (NCB) within its national law enforcement structure. The NCB acts as the primary point of contact between INTERPOL and national authorities, facilitating the exchange of criminal intelligence, digital evidence, operational requests, and other information required for cross-border investigations.

6. REGIONAL OFFICES AND SPECIALISED UNITS

INTERPOL operates several regional offices that support member countries in addressing region-specific security challenges. It also maintains specialised units dedicated to crimes such as cybercrime, terrorism, drug trafficking, financial crime, human trafficking, child exploitation, and environmental crime. These units provide operational support, intelligence analysis, and technical expertise for complex international investigations.

FOCUS AREAS

A.CRIMINAL NETWORKS OPERATING THROUGH ENCRYPTED PLATFORMS

1) EVOLUTION OF TRANSNATIONAL CRIMINAL NETWORKS

Organised criminal groups have increasingly shifted from conventional communication methods to encrypted digital platforms. This transition has enabled them to coordinate activities across multiple jurisdictions with greater secrecy and efficiency. As technology continues to evolve, law enforcement agencies face growing challenges in tracking and disrupting these networks.

2) CRIMINAL USE OF ENCRYPTED PLATFORMS

Encrypted communication platforms have become an important tool for criminal organisations involved in drug trafficking, human trafficking, cybercrime, financial fraud, and terrorism. These platforms allow criminals to communicate securely while reducing the risk of interception. Understanding these evolving methods is essential for developing effective investigative strategies.

3) EMERGING THREATS

Rapid technological advancements continue to create new opportunities for criminal exploitation. Features such as disappearing messages, anonymous communication services, and encrypted file sharing have made investigations increasingly complex. These developments require law enforcement agencies to adapt their investigative techniques continuously.

B.CROSS-BORDER INVESTIGATIONS AND INTERNATIONAL COOPERATION

1) JURISDICTIONAL CHALLENGES

Investigations involving encrypted platforms often extend across multiple countries, creating legal and procedural complexities. Differences in national laws, evidentiary standards, and investigative powers can delay or hinder criminal investigations. Effective cooperation between member states remains essential for addressing these challenges.

2) INTERNATIONAL LEGAL COOPERATION

Mechanisms such as Mutual Legal Assistance Treaties (MLATs), extradition agreements, and bilateral cooperation play an important role in facilitating cross-border investigations. These frameworks enable countries to exchange evidence, intelligence, and other forms of legal assistance. However, procedural delays and differing domestic laws continue to affect their effectiveness.

3) DIGITAL EVIDENCE COLLECTION

Digital evidence has become a key component of modern criminal investigations. Investigators increasingly rely on electronic devices, cloud storage, and communication records to establish links between suspects and criminal activities. Ensuring the lawful collection, preservation, and exchange of such evidence remains a significant challenge.

C. TECHNOLOGICAL CHALLENGES IN INTERNATIONAL INVESTIGATIONS

1) PRIVACY AND PUBLIC SECURITY

Strong encryption has significantly improved digital privacy and cybersecurity. At the same time, it has created challenges for law enforcement agencies attempting to obtain evidence during lawful investigations. Balancing individual privacy with public safety remains a central issue in discussions of encrypted communications.

2) ANONYMOUS TECHNOLOGIES

Technologies that enhance online anonymity have changed the nature of international investigations. Anonymous communication services and privacy-focused digital infrastructure make it increasingly difficult to identify offenders and attribute criminal activity. These developments continue to challenge traditional investigative methods.

3) ILLICIT FINANCIAL NETWORKS

The growing use of cryptocurrencies has transformed the movement of illicit funds across borders. Criminal organisations increasingly exploit digital currencies for money laundering, ransomware payments, and other financial crimes. Strengthening international financial cooperation remains an important aspect of combating these activities.

D. INTERPOL'S ROLE IN STRENGTHENING GLOBAL COOPERATION

1) INTERNATIONAL POLICE COOPERATION

INTERPOL plays a central role in facilitating cooperation between the law enforcement agencies of its member countries. Through its communication systems, databases, and operational support, it enables the timely exchange of criminal intelligence and investigative information. This cooperation is fundamental to addressing transnational crime.

2) OPERATIONAL SUPPORT MECHANISMS

INTERPOL supports member countries through its Notices system, I-24/7 secure communication network, National Central Bureaus, and specialised crime units. These mechanisms assist law enforcement agencies in locating fugitives, sharing intelligence, and coordinating international investigations. They remain vital tools in combating cross-border criminal networks.

3) CAPACITY BUILDING AND FUTURE PREPAREDNESS

As technology continues to evolve, strengthening the capabilities of national law enforcement agencies has become increasingly important. INTERPOL supports member states through specialised training, technical assistance, and the sharing of best practices. Building these capacities helps countries respond more effectively to emerging forms of transnational crime.

Red NOTICE

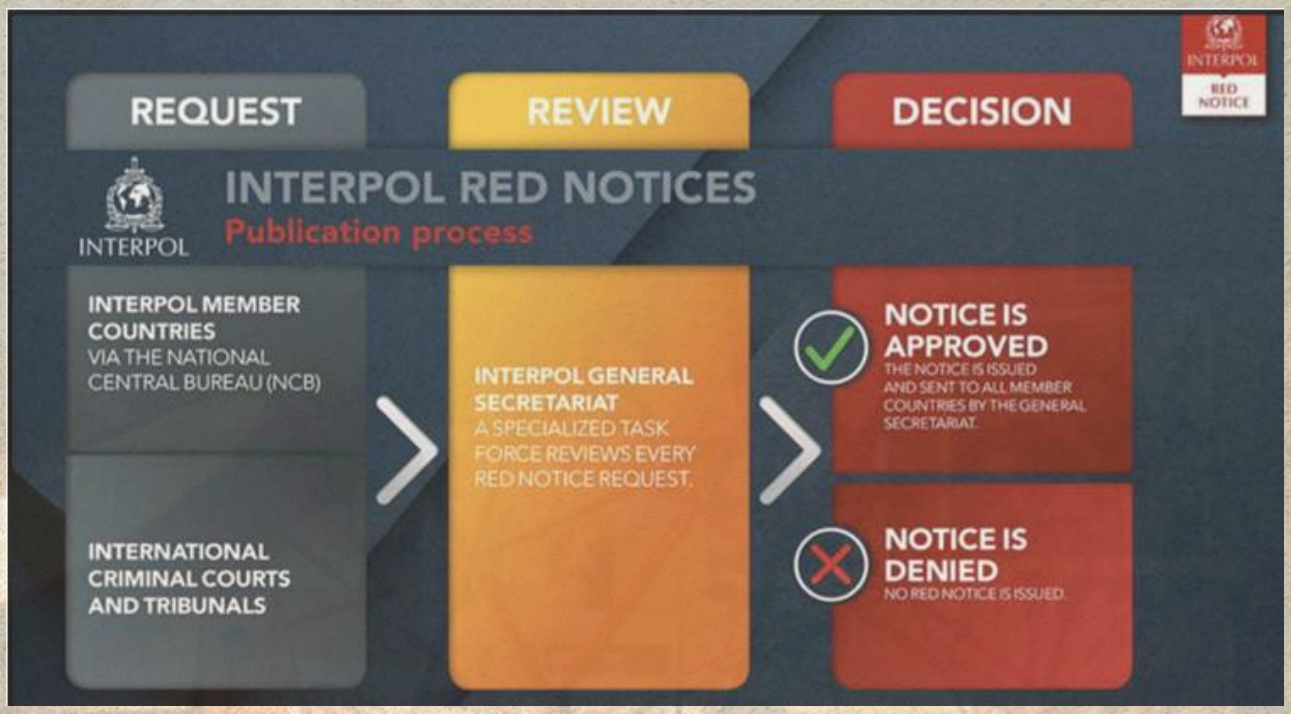
A Red Notice is a request to law enforcement agencies worldwide to locate and provisionally arrest a person pending extradition, surrender, or other legal action. It is not an international arrest warrant; each member country decides whether to act on it in accordance with its domestic laws. Red Notices play a significant role in facilitating cross-border investigations by helping member countries locate fugitives involved in transnational crimes.

The majority of Red Notices are restricted to law enforcement agencies. However, extracts may be made public at the request of the issuing member country, particularly when public assistance is required to locate a fugitive or when the individual is considered a threat to public safety.

A Red Notice generally contains:

- Information used to identify the wanted person, including their name, date of birth, nationality, photographs, fingerprints, and other identifying details, where available.
- Information relating to the offences for which the individual is wanted, including crimes such as terrorism, drug trafficking, cybercrime, human trafficking, financial crime, money laundering, murder, and other serious transnational offences.

INTERPOL publishes Red Notices at the request of a member country or an international tribunal, provided the request complies with INTERPOL's Constitution and the Organisation's Rules on the Processing of Data.


REQUEST
REVIEW
DECISION
INTERPOL
RED NOTICE
INTERPOL RED NOTICES
Publication process
INTERPOL
INTERPOL MEMBER COUNTRIES
VIA THE NATIONAL CENTRAL BUREAU (NCB)
INTERNATIONAL CRIMINAL COURTS AND TRIBUNALS
INTERPOL GENERAL SECRETARIAT
A SPECIALIZED TASK FORCE REVIEWS EVERY RED NOTICE REQUEST.
NOTICE IS APPROVED
THE NOTICE IS ISSUED AND SENT TO ALL MEMBER COUNTRIES BY THE GENERAL SECRETARIAT.
NOTICE IS DENIED
NO RED NOTICE IS ISSUED.

The Other Types of NOTICES

BLUE NOTICE

Purpose: Seeks information about a person's identity, location, or activities to assist in criminal investigations.

Agenda Link: Plays a key role in cross-border investigations by helping member countries locate individuals suspected of operating criminal networks through encrypted communication platforms.

Key Issues:

- Difficulty in identifying suspects using anonymous or encrypted communication services.
- Delays in intelligence sharing across jurisdictions.
- Inconsistent quality and timeliness of information provided by member countries.

Details:

- Issued when law enforcement agencies require additional information about a person of interest.
- Assists in tracking suspects involved in cybercrime, financial crime, trafficking, and other transnational offences.

Yellow Notice

Purpose: Facilitates the search for missing persons or identifying individuals who cannot identify themselves, such as children or vulnerable adults.

Agenda Link: Supports international cooperation in locating missing persons and victims who may have been moved across borders by transnational criminal networks.

Key Issues:

- Cross-border coordination in missing persons investigations.
- Delays in exchanging biometric and identification data.
- Differences in national investigative procedures.

Details:

- Commonly used in cases involving missing children, trafficking victims, and vulnerable persons.
- Supports cooperation between member countries during international investigations.

Black Notice

Purpose: Requests information to identify unknown deceased individuals.

Agenda Link: Assists in identifying victims of transnational crime, trafficking networks, terrorism, and other cross-border criminal activities.

Key Issues:

- Difficulties in identifying victims across multiple jurisdictions.
- Limited forensic capabilities in some member countries.
- Delays in international information sharing.

Details:

- Used in cases involving unidentified human remains.
- Supports forensic cooperation and cross-border victim identification.

Green Notice

Purpose: Warns member countries about individuals who may pose a threat to public safety.

Agenda Link: Enables member countries to share preventive intelligence regarding individuals associated with transnational criminal organisations and cyber-enabled crime.

Key Issues:

- Timely dissemination of preventive intelligence.
- Coordination between national law enforcement agencies.
- Monitoring repeat offenders operating internationally.

Details:

- Used to warn countries about individuals likely to commit offences in multiple jurisdictions.
- Frequently applied in cases involving organised crime, terrorism, and serious violent offences.

Orange Notice

Purpose: Alerts member countries about serious and imminent threats posed by dangerous materials, objects, or methods.

Agenda Link: Supports international efforts to respond to emerging threats, including cyber-enabled attacks targeting critical infrastructure and public safety.

Key Issues:

- Rapid dissemination of threat information.
- Coordination during international emergencies.
- Responding to evolving criminal methods.

Details:

- Used to warn countries about dangerous devices, explosives, hazardous substances, or emerging criminal threats.
- Assists member countries in taking preventive measures.

Purple notice

Purpose: Shares information about criminal methods, concealment techniques, and operating procedures.

Agenda Link: Particularly relevant to this agenda, as it enables member countries to exchange information on how criminal networks exploit encrypted platforms, digital technologies, and other evolving methods.

Key Issues:

- Rapid evolution of criminal techniques.
- Sharing best practices among member countries.
- Keeping investigative methods up to date.

Details:

- Used to circulate information on emerging criminal methodologies.
- Frequently issued in relation to cybercrime, drug trafficking, financial crime, human trafficking, and smuggling.

Silver Notice

Purpose: Assists in tracing, identifying, and locating criminal assets linked to organised crime and other serious offences.

Agenda Link: Supports investigations into the financial activities of criminal networks, including those that use cryptocurrencies and other digital assets to move illicit funds across borders.

Key Issues:

- Tracing illicit financial flows.
- Recovering criminal assets across jurisdictions.
- Cooperation between financial intelligence and law enforcement agencies.

Details:

- Helps identify and recover assets connected to organised crime.
- Supports investigations involving money laundering, financial crime, and cryptocurrency-related offences.

INTERPOL–United Nations Security Council Special Notice

Purpose: Identifies individuals and entities subject to United Nations Security Council sanctions.

Agenda Link: Strengthens international cooperation against individuals and organisations involved in terrorism, sanctions evasion, and other cross-border threats.

Key Issues:

- Consistent implementation of UN sanctions.
- Balancing INTERPOL's neutrality with international obligations.
- Information sharing among member countries.

Details:

- Supports the enforcement of UN Security Council sanctions.
- Assists member countries in identifying sanctioned individuals and entities through INTERPOL's global policing network.

POINTS TO TALK ABOUT

1. Should member states establish an international standard requiring tech companies to build "backdoors" or lawful access mechanisms into End-to-End Encrypted (E2EE) applications?

2.How can law enforcement agencies intercept criminal communications without infringing on the fundamental right to privacy of innocent civilians?

3.What framework can INTERPOL suggest to compel or incentivise private tech companies (like Meta, Telegram, or Signal) to cooperate with international criminal investigations?

4.If encryption is weakened or regulated for law enforcement access, how can the international community guarantee authoritarian regimes won't abuse this access to track journalists, activists, or dissidents?

5.How should law enforcement handle investigations involving decentralised encrypted apps or open-source encryption where there is no central "company" or CEO to subpoena?

6. The current Mutual Legal Assistance Treaty (MLAT) process takes months. How can member states create a standardised, fast-track system for sharing digital evidence in urgent, time-sensitive cases?

7. If a criminal in Country A uses an app developed in Country B, and the data is stored on a cloud server in Country C, whose laws govern the investigation and extraction of that data?

9.What diplomatic or legal mechanisms can be used against "haven" nations that refuse to cooperate with INTERPOL or actively shelter cybercriminal networks?

10.What international standard of evidence or "probable cause" should be required before one country can legally demand decrypted data from another country's servers?

11.How can INTERPOL's I-24/7 global police communications system be modernised to share intercepted digital intelligence in real-time?

12.Should INTERPOL create a formal mechanism to integrate intelligence from private cybersecurity firms (like FireEye or CrowdStrike) into official law enforcement databases?

13.Should INTERPOL establish a permanent, specialised global task force dedicated solely to tracking and infiltrating Dark Web and encrypted criminal syndicates?

14.What universal guidelines should INTERPOL establish for the ethical use of digital forensics tools and spyware (like Pegasus) by member states during investigations?

15.How can INTERPOL better coordinate multi-national "sting" operations (like Operation Trojan Shield/ANOM) where police trick criminals into using compromised encrypted devices?

16.How can developed nations with advanced cyber capabilities (e.g., the USA and the UK) support developing nations that lack the software and training to investigate encrypted networks?

17. What specific programs can the INTERPOL Global Complex for Innovation (IGCI) implement to standardise digital forensics training for police forces worldwide?

18. Should INTERPOL create a centralised "Digital Forensics Hub" where member states lacking resources can send seized encrypted devices (laptops, phones) for expert analysis?

19. How will advanced cyber-training programs and the distribution of decryption software to developing nations be funded within the INTERPOL budget framework?

20. How can global law enforcement agencies prevent the "brain drain" of their best cyber-experts and cryptographers leaving for high-paying jobs in the private sector?

21. Since encrypted platforms are often used in tandem with cryptocurrency, what international protocols are needed to trace and seize crypto-assets moving across borders?

22. How can member states effectively map and dismantle illegal marketplaces on the Dark Web (like the former Silk Road) that use layered encryption (like Tor)?

23. Since breaking E2EE is difficult, how can law enforcement use Artificial Intelligence to analyse "metadata" (who messaged whom, when, and how often) to map criminal networks without reading the actual messages?

24. Are there specific, expedited digital-evidence sharing protocols that should be implemented exclusively for severe crimes like human trafficking or Child Sexual Abuse Material (CSAM)?

25. With the rapid advancement of quantum computing (which could, in theory, instantly break current encryption), what proactive measures should INTERPOL take to prepare law enforcement for the next generation of cyber threats?

Material to go through

- https://journals.sagepub.com/doi/10.1177/0019556124128488 6?icid=int.sj-abstract.si milar-articles.2
- http://eskup.kpu.edu.rs/dar/article/view/663/361
- https://www.tandfonline.com/doi/full/10.1080/13600834.2020.1705035#d1e130
- https://www.jurnalius.ac.id/ojs/index.php/jurnalIUS/article/view/1554/640
- https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060
- https://www.visualcapitalist.com/facial-recognition-world-map/ (Old data)
- https://repository.wodc.nl/server/api/core/bitstreams/6fa89957-53ac-4358-939d-4681d 1b404a0/content