BMUNIS'25 BACKGROUND GUIDE

BMUNIS X INTERPOL

LETTER FROM THE CHAIRS

Greetings to one and all,

We have the honour and pride to welcome you to the esteemed council of INTERPOL (the International Criminal Police Organization), an international body that facilitates worldwide police cooperation beyond the limits of borders. INTERPOL works to combat transnational crime, terrorism, cybercrime, and other serious threats by enabling coordination among law enforcement agencies across its 196 member countries. In this council, we will be addressing two crucial issues, focusing on combating sanctions bypass and tackling major economic offences that challenge global stability and security.

As delegates, you will be expected to be well-versed in your country's stance on the issues, as well as previous solutions implemented and the current situation of the same. It is necessary to note that, as delegates, you're representing a country and, thus, are obliged to defend your allocated delegation's stance, even though it may not align with your personal opinions. Hence, it is necessary that all the delegates remain respectful and diplomatic at all times.

That being said, this background guide has been made to serve as a source of reference. This guide will help the delegates understand the complexity of the issue and the direction in which the council is headed. Nevertheless, delegates must not rely too much on this guide and focus more on their own personal research. Creativity and originality are essential while making your position papers and coming up with ideas for your resolution, so feel free to be innovative and unique in your approach to the same.

Finally, we would like to welcome you to INTERPOL once again. We wish all the delegates all the very best for this MUN as well as for their future ones.

Best Regards,

Chairpersons,

Vikas Vijayan & Karthik Manoj

ISSUE 1: HOW SHOULD INTERPOL ADDRESS SANCTIONS EVASION AND ECONOMIC CRIMES?

INTRODUCTION

One of the most popular diplomatic and economic strategies for preventing human rights abuses, discouraging aggression, and enforcing adherence to international standards is the use of sanctions. But the capacity of governments, businesses, and criminal groups to get around them frequently lessens their impact. Complicated networks of front firms, shell corporations, illegal trade, and financial crimes like fraud and money laundering are frequently involved in sanctions evasion.

This problem poses a challenge as well as an opportunity for INTERPOL. Although it is not a sanctioning body, INTERPOL, a neutral police coordination organization with 196 member nations, is essential to facilitating global collaboration in the fight against financial crime. Effectiveness and neutrality must be balanced in this discussion. How can INTERPOL improve its role in preventing sanctions evasion and associated economic crimes without picking sides in political conflicts?

DEFINITION OF KEY TERMS

- **SANCTIONS** – Restrictions or penalties imposed by states or international organizations to influence behavior or punish violations of international law.
- **SANCTIONS EVASION** – The deliberate act of circumventing sanctions, often through front companies, third-party states, illicit trade, or false documentation.
- **ECONOMIC CRIMES** – Financially motivated, non-violent crimes including money laundering, smuggling, fraud, tax evasion, and corruption.
- **ILLICIT FINANCIAL FLOWS (IFFS)** – Cross-border transfers of money that are illegally earned, transferred, or used.
- **SHELL COMPANIES** – Legally registered firms with little or no operations, often used to conceal ownership or evade sanctions.
- **INTERPOL NOTICES** – International alerts issued by INTERPOL, such as:

- RED NOTICE (WANTED PERSONS)
- PURPLE NOTICE (CRIMINAL MODUS OPERANDI)
- BLUE NOTICE (COLLECTING INFORMATION)

GENERAL OVERVIEW

The international community consistently relies on sanctions as a non-military means of combating human rights violations, punishing sovereignty infractions, deterring terrorism, and enforcing adherence to international norms. They can go after whole states, particular sectors of the economy, or people and organizations. However, increasingly complex evasion strategies, frequently made possible by global economic crimes, are undermining their efficacy.

NATURE OF SANCTIONS AND THEIR ROLE

SANCTION TYPES:

- Comprehensive sanctions completely prohibit trade, finance, and diplomacy (as was the case with Iraq in the 1990s).
- “Smart" or targeted sanctions impose limitations on particular people, businesses, or industries (e.g., banking and energy sanctions on Iran).
- Purpose: Restrict access to international systems, compel governments to alter their actions, and limit a state's ability to finance illegal activity.

HOW SANCTIONS ARE EVADED

FINANCIAL MANIPULATION:

- Ownership is concealed through the use of offshore banking and shell corporations.
- Money laundering to cover up the source of illegally obtained funds.
- Utilizing cryptocurrencies to bypass traditional financial channels.

TRADE-BASED EVASION:

- Smuggling across porous borders.
- Oil and cargo are transferred from ship to ship at sea.
- Flags of convenience, in which vessels register as neutral to evade detection.

THIRD-PARTY INVOLVEMENT:

- Prohibited trade is carried out through neutral corporations or proxy states.

For instance, items are being rerouted through middlemen in nations with less strict enforcement by sanctioned governments.

ECONOMIC CRIMES TIED TO SANCTIONS EVASION

- Bribery and corruption: authorities who are bribed to ignore banking or customs irregularities.
- False shipping manifests, re-labelled items, and phony invoices are examples of fraudulent documentation.
- Illicit Financial Flows (IFFs): earnings that are transferred into foreign accounts or put back into respectable companies in an effort to "clean" up funds.

WHY THIS MATTERS FOR INTERPOL

IMPACT ON GLOBAL SECURITY:

- Avoiding sanctions damages international law's credibility.
- Illicit revenues have the potential to support organized crime, terrorism, and the trafficking of weapons.

NEUTRALITY CHALLENGE:

- Sanctions are fundamentally political, even though Interpol is not a political organization.
- Interpol must combat economic crime without coming seen as biased in favour of the sanctioning authorities.

OPERATIONAL RESTRICTIONS:

- Interpol depends on member states' assistance and is unable to impose sanctions directly.
- Globally, varying levels of political will lead to uneven enforcement.

CURRENT TRENDS AND GROWING CONCERNS

- New avenues for evading sanctions are made possible by the growth of cryptocurrencies and digital finance.
- More and more state and non-state actors are using complicated, hard-to-trace global networks.

- Because of ongoing geopolitical disputes (such as those involving North Korea, Iran, and Russia), sanctions will continue to be a major diplomatic instrument, making evasion a persistent problem.

MAJOR PARTIES INVOLVED

UNITED STATES & EUROPEAN UNION – Lead sanctioning bodies with strong compliance frameworks.

UN SECURITY COUNCIL (UNSC) – Issues binding sanctions under international law.

RUSSIA, IRAN, NORTH KOREA – Major sanctioned states, often accused of evasion.

CHINA & TURKEY – Countries accused of indirectly facilitating sanctioned trade.

FINANCIAL ACTION TASK FORCE (FATF) – Sets global standards for anti-money laundering and counter-terrorism financing.

PRIVATE SECTOR (BANKS, CORPORATIONS, SHIPPING) – Critical in compliance and detection.

INTERPOL MEMBER STATES – Varying levels of willingness to enforce and cooperate.

TIMELINE OF KEY EVENTS

1980S – Sanctions against apartheid South Africa highlight enforcement challenges.

1990s – Iraq sanctions reveal humanitarian impacts and widespread evasion.

2001 – Post-9/11, financial monitoring and counter-terrorism financing strengthened.

2010S – Iran and North Korea sanctions bring focus to complex evasion networks.

2014 – Western sanctions on Russia following Crimea annexation increase global debate.

2022 – Russia's invasion of Ukraine sparks the largest sanctions regime in history, exposing major evasion routes.

2023-PRESENT – INTERPOL expands work with FATF and launches the Financial Crimes and Anti-Corruption Centre (IFCACC).

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

- UN Sanctions Committees do oversee compliance, however, do not carry out enforcement.
- FATF Recommendations carry out defining procedures on FA and AMLA compliance.
- Interpol Initiatives - Track criminal techniques with Purple Notices Using IFCACC as a central point for financial crime.
- European Union, World Customs Organization, and INTERPOL work together on cross-border crime.
- AI, blockchain oversight, and guidelines for tighter banking enforcement have been adopted.

CHALLENGES

- Geopolitical rivalries hinder collaboration.
- Certain jurisdictions evade penalties, and the enforcement of any penalties becomes beneficial.
- Gaps in regulation on offshore banking and inadequate jurisdictions leads to a collapse of the control system.

POSSIBLE SOLUTIONS

MODERNIZED INFORMATION EXCHANGE

- Different parties must incorporate on an INTERPOL maintained central database for sanctioned and flagged individuals, companies, and vessels.
- Further enhance collaboration with the FATF, private banks, and Europol.

INSTRUCTIONAL DEVELOPMENT

- Train weaker economies on financial crime analysis.
- Provide additional assistance for monitoring the misappropriation of cryptocurrency.

SYSTEMS INTEGRATION

- Monitor financial flows and trade using blockchain to trace technology.

- Implement AI systems to analyze and highlight potentially fraudulent transactions.

CHANGED APPROACH TO INTERPOL'S NEUTRALITY

- Restrict monitoring of INTERPOL'S politically active member states to information sharing and crime detection.
- INTERPOL's technical division should maintain technical neutrality to the organization.

INCREASED ACCOUNTABILITY

- Encourage states to require the public disclosure of the true owners of companies.
- Enhance monitoring of the shipping register to eliminate flag of convenience abuses.

BIBLIOGRAPHY

- https://www.unodc.org/unodc/en/money-laundering/index.html
- https://www.fatf-gafi.org
- https://www.interpol.int/en/Crimes/Financial-crime
- https://www.cfr.org/backgrounder/sanctions-evasion
- https://www.reuters.com/world/russias-shadow-fleet-oil-tankers-2023-03-16/
- https://carnegieendowment.org/politika/iran-sanctions-evasion
- https://www.transparency.org/en/
- https://www.interpol.int/content/download/12626/file/Repository%20of%20practice%20Articles%202%20and%203.pdf
- https://www.interpol.int/en/Crimes/Corruption/Anti-corruption-and-asset-recovery
- https://g20.utoronto.ca/2020/Scoping_Paper_on_International_Cooperation_04092020_V4_final.pdf
- https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/bribery-corruption-and-sanctions-evasion

ISSUE 2: REGULATING CROSS-BORDER CRYPTOCURRENCY FRAUD & INTERPOL REFORM

INTRODUCTION:

Originally hailed as a ground-breaking development in financial technology, cryptocurrencies have also been used by criminals as a means of money laundering, fraud, and illegal transfers. There are now significant gaps for criminals to take advantage of due to the lack of an internationally coordinated regulatory framework. Some nations have strict anti-money laundering (AML) and know your customer (KYC) laws, while others have little to no regulation.

Although organizations like the Financial Action Task Force (FATF) have tried to offer guidelines, their actions are not legally obligatory, and various governments implement them differently. Jurisdictional uncertainty is encouraged by this fragmented approach: an offender may be in one nation, his or her victim in another, and the criminal proceeds laundered through several blockchain networks in a matter of seconds.

The worldwide response should change along with blockchain technology. As the biggest international police agency in the world, Interpol can help member governments work together to stop these kinds of scams involving cryptocurrency. But Interpol itself is vulnerable to criticisms and structural flaws that highlight the need for change.

DEFINITION OF KEY TERMS:

- **CRYPTOCURRENCY**: A digital or virtual currency secured by cryptography, operating on decentralized blockchain networks.
- **BLOCKCHAIN**: A distributed ledger technology that records transactions on numerous computers, with data difficult to alter retroactively.
- **KNOW YOUR CUSTOMER (KYC)**: Regulations that force cryptocurrency exchanges and financial institutions to verify their customers' identities.

- **ANTI-MONEY LAUNDERING (AML):** Regulations, laws, and policies that aim at preventing criminals from making illegally gained money look like legitimate earnings

- **FINANCIAL ACTION TASK FORCE (FATF):** An intergovernmental agency that develops suggestions to combat money laundering, terrorist financing, and other threats.

- **RUG PULL:** A scam in which developers deceive investors by abruptly withdrawing cash from a cryptocurrency project.

- **JURISDICTIONAL ARBITRAGE:** Exploiting differences in national law or regulatory loopholes to avoid prosecution or oversight.

- **MIXERS/TUMBLERS:** Services that combine cryptocurrency from numerous users and then re-distribute it to new addresses in smaller, randomly chosen amounts. Criminals frequently use this procedure to launder money or cover up the trail of stolen assets because it makes it difficult to determine the original source of funds.

GENERAL OVERVIEW

1. CRYPTOCURRENCY FRAUD ON THE RISE:

Cryptocurrency has grown significantly, with its global market capitalization reaching a high of over $2 trillion. With legitimate usage, fraud has also grown. Victims are typically retail investors who have been lured by unrealistic returns, and perpetrators exploit the anonymity and global reach of blockchain networks.

2. FRAUD TYPICALLY OCCURS IN THE FOLLOWING FORMS:

- **INVESTMENT SCAMS & PONZI SCHEMES:** Victims are lured by scammers offering "guaranteed returns".
- **PHISHING & IDENTITY THEFT:** Users are tricked by offenders into revealing private keys.
- **EXCHANGE HACKS & FAKE PLATFORMS:** Under-regulated or false exchanges disappear with funds.
- **RUG PULLS:** Developers abandon projects after getting investments.

JURISDICTIONAL CHALLENGES:

Immediate cross-border cryptocurrency transactions enable scammers to target victims anywhere in the world. Coordination between law enforcement is quite challenging due to the lack of centralized controls and diverse national rules.

3. REGULATORY FRAGMENTATION:

Rules and regulations for cryptocurrencies in many countries are different too, significantly contributing to an increase in crypto-related scams. For example,

- Certain countries (e.g., the U.S.) treat cryptocurrencies as commodities or securities and regulate them accordingly.
- Others (e.g., Japan, Singapore) have strict regulatory regimes with mandatory licensing.
- There are countries (e.g., emerging economies) with no official crypto legislation whatsoever.
- This inconsistency makes it easy for criminals to exploit "weak links" in global regulation by committing jurisdictional arbitrage.

4. INTERPOL'S ROLE:

Interpol has launched programs such as the Global Complex for Innovation (IGCI) in Singapore, and cybercrime units that track online fraud (specifically crypto scams). Interpol, however, has limited authority—it cannot directly prosecute crimes but must rely on cooperation from member countries. Allegations of political misuse of Interpol red notices and slow reaction to emerging trends of cybercrime indicate the need for reform.

MAJOR PARTIES INVOLVED:

- **UNITED STATES:** The USA is a global leader in crypto enforcement and regulation, with the SEC, CFTC, and DOJ actively pursuing crypto market manipulation and fraud. It is also engaged in international cooperation for following cross-border criminal funds.

- **UNITED KINGDOM:** The UK regulates crypto companies through the Financial Conduct Authority (FCA), emphasizing AML/KYC requirements and

protection of investors. It is actively following up on fraudulent websites and promotional scams.

- **EUROPEAN UNION**: Leading European regulators have strong crypto exchange licensing frameworks. Countries like France and Germany have consumer protection and enforcement priorities, while countries like Switzerland strike a balance between regulation and innovation.

- **JAPAN:** Japan has stringent enforcement against fraudulent exchanges and mandatory AML/KYC regulations for transparent crypto licensing.

- **SINGAPORE:** Singapore prioritizes investor protection and transparency through strict crypto rules and exchange licensing.

- **RUSSIA:** There is partial regulation for the usage of cryptocurrencies in Russia, but loopholes enable illegal activity. Enforcement is patchy, and some use the country as a hub for cross-border crypto activity.

- **CHINA:** Exchanges and mining are prohibited across most of crypto activity in China, but illegal activity continues under tight state control.

- **INDIA:** India has a Rapidly evolving crypto space with maturing licensing frameworks and focuses on increasing enforcement against frauds and illegal exchanges.

- **NIGERIA:** Due to remittances, inflation, and restricted access to traditional banking, Nigeria has one of the highest rates of cryptocurrency adoption in the world. However, it also faces a lot of fraud, Ponzi schemes, and scams that target individual investors.
- **MEXICO:** Mexico has focused on strengthening crypto regulation, including exchange registration and consumer protection, as it battles fraud.

- **UAE:** The UAE has helped promote innovative exchange and crypto firm licensing, attempting to make the region a hub for crypto innovation while applying AML/KYC regulations.

- **TÜRKIYE:** Türkiye's regulatory approach remains nonsystemic; government has implemented restrictions on crypto payment while imposing some reporting requirements on exchanges.

- **IRAN:** Iran has adopted cryptocurrency mining as a means of getting over economic sanctions, and state-sponsored businesses are a major contributor to the Bitcoin network. It has also taken tough measures against illegal mining and is accused of utilizing cryptocurrency to evade sanctions.

TIMELINE OF EVENTS:

2009: The first decentralized cryptocurrency, Bitcoin, was introduced.

2011–2013: The use of cryptocurrency in illegal trade is made more common by darknet marketplaces such as Silk Road.

2014: The collapse of the Mt. Gox exchange, which cost $450 million, revealed weaknesses in cryptocurrency exchanges.

2018: The FATF revises its rules to incorporate cryptocurrencies into AML frameworks.

2019: To combat crimes involving cryptocurrency, Interpol works with cybersecurity companies.

2020–2021: These years saw an increase in ransomware attacks and scams requesting cryptocurrency payments.

2022–2024: Coordinated international takedowns start; "pig-butchering" scams increase.

PREVIOUS ATTEMPTS TO RESOLVE THE ISSUE:

FATF GUIDELINES (UPDATED IN 2018 AND 2019): This introduced the "Travel Rule" which mandates that crypto exchanges share user data. However, its implementations vary regionally.

INTERPOL CYBERCRIME INITIATIVES: Interpol has introduced specialized units in Singapore and Lyon to monitor fraud related to cryptocurrency. However, their efficacy is dependent upon member states' cooperation.

NATIONAL REGULATIONS: While not widely embraced, nations such as the EU, Singapore, and Japan have established robust licensing frameworks against crypto-fraud or scams.

PUBLIC-PRIVATE PARTNERSHIPS: A handful of blockchain analytics companies have begun cooperating with law enforcement to facilitate investigations. However, there is still an imbalance in the sharing of data.

POSSIBLE SOLUTIONS:

1. ENHANCING INTERPOL'S CAPABILITIES:

- Form a task force specifically focused on cryptocurrency crime.
- Increase the speed at which private companies and member states exchange information.
- Reform governance to increase transparency and responsiveness.

2. INTEGRATION OF GLOBAL REGULATIONS:

- Promote the FATF guidelines' acceptance as legally binding international norms.
- Decide on uniform cryptocurrency definitions and classifications.

3. MECHANISMS OF JURISDICTIONAL COOPERATION:

- Create international agreements that specify authority over global cybercrimes.
- Adopt quick response procedures to stop illegal money transfers.

4. PUBLIC AWARENESS & EDUCATION:

- Start international campaigns to educate users about the risks of cryptocurrencies.
- Exchanges should be required to give explicit warnings about high-risk products.

5. COOPERATION IN TECHNOLOGY:

- Work together with blockchain analytics firms to identify fraudulent activity.
- Create shared databases for addresses and wallets that seem suspect.

APPENDIX

1. **CASE STUDY** – Mt. Gox (2014): What had been the largest Bitcoin exchange in the world, Mt. Gox, was destroyed by losing over 850,000 BTC, most of

which were stolen and mishandled. This case highlighted how unregulated exchanges can result in massive fraud and loss to investors.

2. **CASE STUDY** – OneCoin Scam (2014–2017): Billed as a legitimate cryptocurrency, OneCoin was later discovered to be a multi-billion-dollar Ponzi scheme. Its collapse brought to the fore the necessity of public awareness and government intervention in combating fraud.

3. **CASE STUDY** – PlusToken Scam (2019): The scam, which originated from China, had investors of over $2 billion worth of cryptocurrency. It then became a case study on how large-scale fraud can function over borders with little enforcement in the near term.

4. **CASE STUDY**-The 2019 QuadrigaCX Scandal: Following the sudden death of its creator, Gerald Cotten, QuadrigaCX went bankrupt, rendering $190 million in customer assets unusable. The dangers of centralized management and inadequate oversight were exposed by investigations that showed Cotten had consistently stolen client funds, operating a Ponzi scheme.

5. **HIGH-PROFILE ENFORCEMENT ACTION** – BitMEX (2020): The U.S. charged BitMEX, a top-ranked crypto derivatives exchange, with failing to have AML and KYC procedures in place. This enforcement action highlighted how regulators are beginning to hold exchanges accountable for failure to comply.

BIBLIOGRAPHY

- Mt. Gox Scandal – Wikipedia: https://en.wikipedia.org/wiki/Mt._Gox
- QuadrigaCX Scandal – Wikipedia: https://en.wikipedia.org/wiki/Quadriga_(company)
- Cryptocurrency Crime – Interpol: https://www.interpol.int/en/News-and Events/News/2021/Cryptocurrency-crime-preventing-the-misuse-of-virtual-assets-by-organized-crime-for-money-laundering
- Virtual Assets – Financial Action Task Force (FATF): https://www.fatf-gafi.org/en/topics/virtual-assets.html

- Cryptocurrency Investment Fraud – Federal Bureau of Investigation (FBI): https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud

- Money Laundering through Cryptocurrencies – United Nations Office on Drugs and Crime (UNODC): https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html

- What to know about Cryptocurrencies and Scams – Federal Trade Commission (FTC): https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams

- Tackling Crypto Crime and Money Laundering – Basel Institute on Governance: https://baselgovernance.org/news/seizing-opportunity-europol-basel-institute-recommendations-tackling-crypto-crime-and-money

- Cryptocurrency and Pig Butchering Scams – CNBC: https://www.cnbc.com/2025/02/13/crypto-scams-thrive-in-2024-on-back-of-pig-butchering-and-ai-report.html