MLRIT
Raising Engineers

MLRIT MUN 2025

BACKGROUND GUIDE.

MLRIT MUN

Model United Nations

UNODC.

mlritmun@mlrit.ac.in

mlrit_mun

MLRIT MUN
Model United Nations

COMMITTEE : UNODC

UNODC.

Agendas:

Agenda: Developing a Coordinated Global Response to the Technological Evolution of Financial, Drug, and Terror Networks.

Disclaimer: : The authors of the document do not claim any copyright over it. All the details, information, and content mentioned in the document is only for educational purpose under the 'fair use' policy. The content established below is in no way related to the personal ideologies of the Executive board. This background guide is authored with a sole intention of giving delegates a direction in the committee and orient them on the avenues of research.

Table Of Contents.

Message From The Secretary General.

Dear Delegate,

If you're nervous, good. It means you care. Every great speaker, every confident diplomat, started right where you are: unsure, curious, and ready to learn. But at MLRITMUN, we don't wait for confidence to arrive; we build it.

This edition is more than debate and diplomacy. It is a space where ideas collide, voices rise, and leaders take shape. Here, you'll learn to think fast, speak with clarity, and solve problems that demand both logic and courage. You'll find mentors who guide you, peers who challenge you, and moments that transform you.

When the gavel strikes, remember it's not about being perfect. It's about being fearless. If you're backed against a wall, break the whole goddamn thing down. Don't wait for luck; make your own.

At MLRITMUN 2025, every delegate has a chance to rise. Speak. Challenge. Lead. Because this isn't just another conference. It's where your voice begins to matter.

And when it does, I'll be right there watching, guiding, and cheering you on.
I'll see you on the other side of the gavel.

With conviction,
Khaja Moizuddin
Secretary-General,
MLRITMUN 2025 | 7th Edition

Letter From The Executive Board.

Delegates, Congratulations on taking the bold step to decide to delegate at MLRITMUN 2025.

We are looking forward to working with you all and ensuring a constructive debate. We hope that this simulation proves fruitful to you and you take something valuable back from it.

We aim at giving you a better and thorough insight upon the working and functioning of The UN and its sub-committees. We also hope that by the end of the conference you will have a better understanding about the procedures, rules and objectives and that you will be willing to participate in more such MUN's.

We have designed a Background Guide for you to start off your research process. The Background Guide is a major resource for you but should not provide a hindrance in your external research. The Background Guide will help you get familiar with the agenda..Its background but for the committee to progress as a delegate you must carry forward external research. The Background Guide will provide you with very basic and guiding insights. Do not base off all of your research from this guide.

As mentioned, this is just the basics. For your external research and background research on your country, you are advised to research like there's no tomorrow!

We urge all members of the committee to take the time to read the background guide and use it as a starting point for their preparation. We urge every delegate to come to the conference with an open mind, ready to meet and work with new people, and actively participate in the debate in the committee, debate and argue solutions and problems and help form a thorough and effective resolution.

The Executive Board looks forward to your presence at MLRIT!

Happy MUNning and Researching!

Best Regards,

Faraazuddin (Chairperson)

Soha Afneen (Vice-Chairperson)

Agenda: Developing a Coordinated Global Response to the Technological Evolution of Financial, Drug, and Terror Networks

1. Introduction to the Agenda:

The agenda is “Developing a Coordinated Global Response to the Technological Evolution of Financial, Drug, and Terror Networks”, as delegates we should aim to explore how rapid technological change has reshaped the ways in which organized crime operates across borders, because today, financial crimes, drug trafficking, and terrorism are not isolated problems. They have become interconnected through digital tools such as encrypted communication, online financial systems, and artificial intelligence. This convergence has created a new kind of threat that can no longer be addressed by traditional law enforcement alone. The UNODC plays a central role in tackling this issue. Its mandate includes combating illicit drug trafficking, organized crime, corruption, and terrorism, all of which are increasingly dependent on technology. By supporting states in strengthening laws, improving data-sharing, and enhancing digital capacity, the UNODC helps countries adapt to this evolving threat landscape.[1]

This issue matters today because technology has blurred the line between national and transnational crime.

Criminals now use cryptocurrency to launder drug money, social media to recruit for extremist causes, and dark web marketplaces to trade weapons and synthetic drugs. These digital tools make crimes cheaper, faster, and harder to trace. Without coordinated international action, global governance risks falling behind, allowing criminal networks to exploit legal and technological loopholes.

2. Understanding the Core Concepts around this Agenda:

What is the Meaning of "Technological Evolution" in Crime Networks?

The word technological evolution in crime networks refers to the shift from physical, person-to-person methods of committing and financing crimes to sophisticated, technology-driven systems. For example, what once required a courier carrying cash across a border can now be done instantly through blockchain transactions. Similarly, where traffickers once relied on face-to-face meetings, they now use encrypted messaging applications and virtual private networks to communicate securely[1]. Technology does not merely support these activities; it transforms them by enabling anonymity, speed, and global reach.

So, what is the Nexus Between Financial, Drug, and Terror Activities?

Because technology acts as both a tool and a multiplier of criminal capacity, the demand for a coordinated and adaptive global response is felt.
The nexus between financial, drug, and terror activities arises because all three depend on shared infrastructures for movement of money, goods, and information. Drug cartels fund their operations through illicit financial networks; terrorist groups depend on smuggling routes used by drug traffickers; and financial crimes such as money laundering make both possible.[1]

This interdependence has made it difficult to address one form of crime without confronting the others.
Internationally, several case examples highlight how technology reinforces transnational crime. The use of cryptocurrencies such as Bitcoin has facilitated the laundering of drug proceeds and the financing of terrorism without passing through the formal banking system[2]. Dark web platforms like the now-defunct Silk Road enabled anonymous sales of narcotics and weapons, and simultaneously social media algorithms have been exploited for recruitment by extremist groups.

So finally, how does Technology reinforce Transnational Crime?

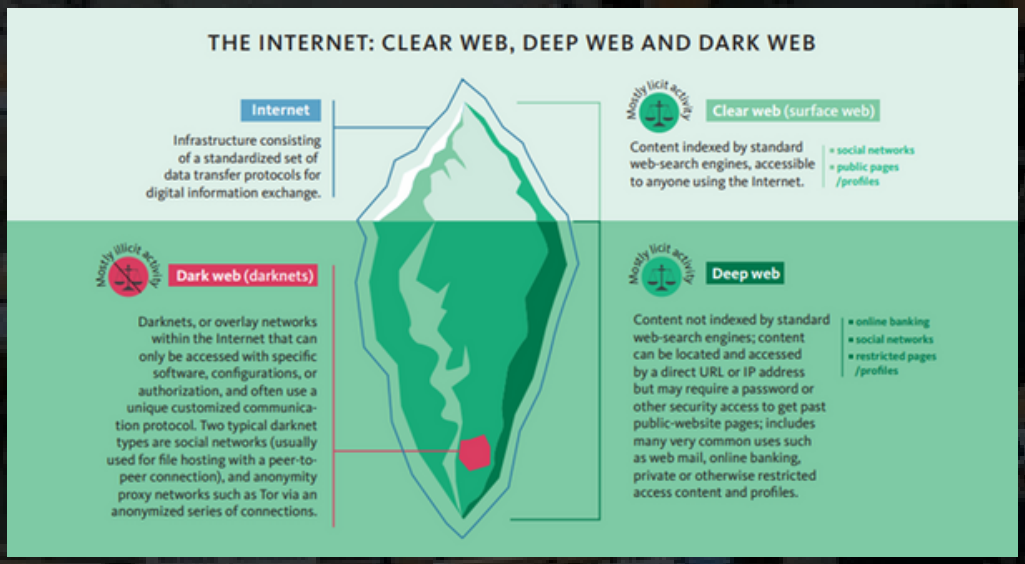
One of the clearest examples of how technology strengthens transnational crime is the rise of cryptocurrency-based money laundering.

One of the clearest examples of how technology strengthens transnational crime is the rise of cryptocurrency-based money laundering. Unlike traditional bank transfers, cryptocurrency transactions can be carried out anonymously across borders, allowing criminals to move large sums of money without relying on regulated financial institutions. Drug cartels and terrorist financiers have used digital wallets and privacy-focused coins to conceal the origin of illicit funds. In 2021, the UNODC reported that over1.5 percent of global cryptocurrency transactions were linked to criminal activity, including drug sales on dark web markets and terror financing[1].

Another important case involves the dark web, a hidden layer of the internet accessible only through special browsers such as Tor. Platforms like Silk Road and AlphaBay became global markets for narcotics, weapons, and forged documents[2].

These platforms used anonymous communication and cryptocurrency payments, making detection and prosecution extremely difficult. Even after their shutdown, similar websites have reappeared, showing how easily these networks adapt.

Technology has also facilitated online recruitment and radicalization. Terror organizations have turned to encrypted platforms such as Telegram and social media channels to recruit followers, share propaganda, and coordinate operations



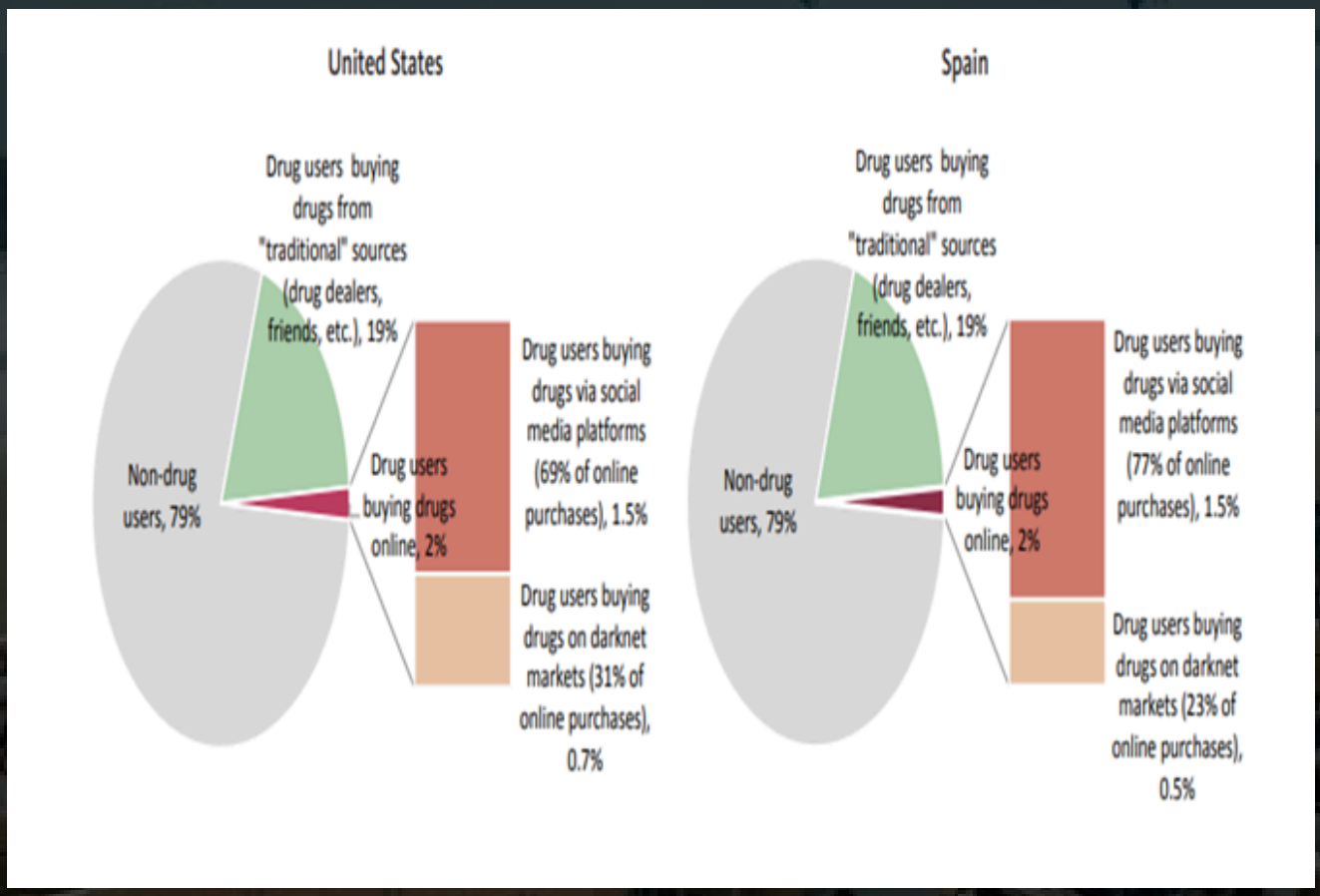
Pictorial Representation of Levels of the Internet,
Source: World Drug Report, 2023

The digital environment allows them to reach individuals across different countries and build transnational networks without physical presence. This use of technology not only lowers the cost of recruitment but also allows terrorist groups to maintain resilience despite international counter-terrorism efforts.

Similarly, synthetic drug production has evolved through technological innovation. Criminal organizations now use digital supply chains, online precursors markets, and automated laboratory setups[1]. For example, the global trade in fentanyl and methamphetamine precursors has moved online, with chemicals sourced through e-commerce channels and payments made in cryptocurrency, this is usually why such methods make law enforcement intervention harder because each step of the process is spread across multiple jurisdictions.

In all these cases, technology amplifies criminal operations by enhancing anonymity, efficiency, and reach, so we need to understand that the same qualities that make digital systems useful for global trade and communication are also at the same time being exploited to evade regulation and expand criminal enterprise.
This has led to a new form of digital transnational crime that cannot be tackled by any single nation-state acting alone. The FATF notes that a coordinated, technology-aware response is therefore essential to safeguard financial integrity, public safety, and international peace, but the larger question we face is: how on earth is it even possible to bridge such gaps?

In Pic: Use of traditional sources versus online purchases of drugs among Internet-using drug users aged 15–25, the United States and Spain



Financial Networks

The global financial system has become the backbone of organized criminal activity. What used to be limited to informal money couriers or underground banking has evolved into a complex digital architecture that combines traditional offshore mechanisms with emerging cryptocurrency ecosystems. The technological shift has multiplied both the speed and the invisibility of financial crimes.

A) The Rise of Cryptocurrency and Digital Money Laundering

Cryptocurrencies have revolutionized how criminal proceeds are moved and disguised. While blockchain technology was designed to promote transparency, the use of privacy coins (such as Monero or Zcash), crypto mixers, and decentralized exchanges now enables near-perfect anonymity[1] Criminal networks convert illicit cash into cryptocurrency, transfer it through multiple wallets, and reintroduce it into the economy through fake e-commerce transactions or peer-to-peer trading platforms.

UNODC has reported that drug cartels in Mexico and Southeast Asia have increasingly used stablecoins such as USDT to bypass volatile exchange rates and avoid detection by financial intelligence units[2]. Once the funds are “layered” through these transactions, tracing them back to their criminal origin becomes nearly impossible. Unlike banks, which are subject to due diligence and suspicious transaction reporting requirements, decentralized crypto networks operate without a central authority, creating a legal vacuum that international law has yet to fill.

A) Case Study: The “Crypto Cartels”

In 2022, Europol and the UNODC uncovered networks known as “Crypto Cartels” operating between Colombia, Spain, and Hong Kong[1]. These groups laundered millions of dollars in cocaine profits through cryptocurrency exchanges that lacked robust Know Your Customer (KYC) compliance. Funds were first converted into Bitcoin, then into stablecoins, and finally cashed out through Hong Kong-based shell firms. The investigation revealed how traditional drug cartels are merging with cybercriminal infrastructure how they exploited blockchain analytics to disguise movement patterns and exploit regulatory fragmentation, lol.

Terror Networks

Technology has restructured the foundations of terrorist financing, recruitment, and propaganda. Terror groups now function as decentralized digital ecosystems where ideology, funding, and coordination intersect online. Terror organizations such as ISIS and Al-Qaeda use digital media to build influence and legitimacy[1].

Through Telegram channels, encrypted chat rooms, and social media algorithms, these groups spread extremist narratives, targeting isolated or disaffected individuals across continents. Their propaganda operations use high-quality video editing, multilingual outreach, and viral marketing strategies modeled on corporate digital campaigns.

Parallel to this, crowdfunding and cryptocurrency have become key tools for financing operations. Small donations through platforms masked as humanitarian or religious

causes are converted into Bitcoin or stablecoins, allowing funds to flow undetected[1]. Law enforcement faces the unique challenge of distinguishing between legitimate online fundraising and covert terror financing in a borderless, anonymous digital environment.

Where is the Intersection betweeen Terrorism & Drug Trafficking?

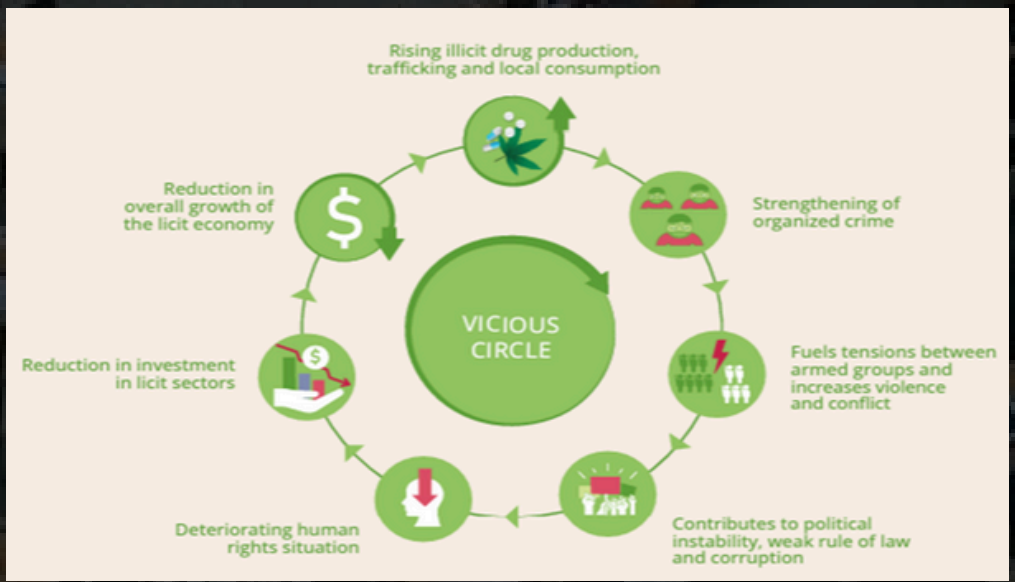
In several regions, terrorism and drug trafficking are deeply linked. Groups such as the Taliban, Hezbollah, and the Revolutionary Armed Forces of Colombia (FARC) have long used narcotics to sustain operations[1]. Technology has reinforced this connection. Terrorist factions use encrypted channels to coordinate with drug traffickers, online money transfer systems to manage profits, and cryptocurrency to store value. The resulting hybrid economy merges ideological and criminal motives, complicating international responses.

The ISIS Case Study

Back then, ISIS remained one of the most technologically adaptive terror organizations. Its members developed encrypted recruitment portals, digital propaganda studios, and online marketplaces to sell looted artifacts and collect ransom payments[1]. In 2020, the U.S. Department of Justice dismantled an ISIS-linked donation network that used fake charity websites and QR-coded crypto wallets to fund militants in Syria[2].

The network demonstrated how terrorism today depends less on physical sanctuaries and more on digital resilience. Even under heavy surveillance, ISIS adapted by shifting its propaganda to decentralized platforms, using cloud storage, VPNs, and mirror websites to avoid detection.

Reader's Note: The Vicious Cycle of represents how all factors are deeply interlinked and intertwined.



Source: UNODC, World Drug Report of 2023

Global Coordination Challenges

The core legal instruments governing transnational crime, such as the UNTOC and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances were drafted before the digital revolution[1]. These frameworks do not directly address emerging technologies such as cryptocurrencies, darknet operations, or artificial intelligence.

Many national laws still define crimes like money laundering or cyber fraud in territorial terms, while digital crime transcends borders[2]. Mutual Legal Assistance Treaties (MLATs) are slow and bureaucratic, often requiring months for a single data request. The lack of real-time data exchange between jurisdictions enables organized crime to exploit time gaps in enforcement[3]. Private technology companies now hold much of the data necessary for investigations. Without international standards mandating cooperation, access to encrypted communications and blockchain records often depends on voluntary disclosure. This imbalance between state authority and corporate control over information has become one of the defining challenges in modern law enforcement.So, naturally, there is need for cyber norms and regulatory cooperation, which means that states that have adopted numerous cybersecurity instruments, need to understand that there is still no unified global agreement defining “responsible behavior” in cyberspace

Divergent national regulations on digital privacy, data retention, and crypto governance create loopholes that criminals exploit. For example, as seen abovea cryptocurrency exchange licensed in one jurisdiction may operate in another with weaker anti-money-laundering (AML) laws, undermining coordinated regulation.

Role of Regional Actors like INTERPOL, FATF, etc.

The fight against technologically enabled transnational crime depends on coordination between specialized international bodies. Interpol operates as a hub for global police cooperation, maintaining databases on digital fingerprints, cryptocurrency wallets, and dark web profiles[1]. However, its effectiveness depends on the willingness of member states to share intelligence promptly.

The Financial Action Task Force develops global standards for countering money laundering and terrorist financing, including specific recommendations on virtual assets and virtual asset service providers (VASPs)[2]. Yet enforcement remains inconsistent, with many jurisdictions still lacking the capacity to monitor decentralized financial systems

[1] Interpol, Global Policing Strategy for Cybercrime (2022)

[2] Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs (2023)

The UNODC serves as the principal UN body coordinating responses to organized crime and drug trafficking. It supports states through legislative guidance, capacity-building, and inter-agency cooperation platforms[1]. The Cybercrime Convention Committee and Global Programme on Cybercrime are examples of UNODC initiatives designed to harmonize responses, but resource disparities between developed and developing countries continue to limit full global alignment.

Existing International Frameworks

Despite the complexity of the threat landscape, several established legal and institutional frameworks form the foundation for international cooperation. These frameworks are essential for aligning national legislation and promoting interoperability between law enforcement agencies.

Role of Regional Actors like INTERPOL, FATF, etc.

The United Nations Convention against Transnational Organized Crime (2000), known as the Palermo Convention, remains the cornerstone of global efforts to combat organized crime[1]. It obliges states to criminalize participation in organized criminal groups, money laundering, and obstruction of justice, and to enhance mutual legal assistance.

. However, the Convention's provisions require modernization to address digital tools used in money laundering and cyber-facilitated trafficking. The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), or Vienna Convention, laid the foundation for cooperation against drug trafficking[1].

It recognized the need for cross-border coordination but did not anticipate synthetic drug production or online trade. The United Nations Convention against Corruption (2003) also complements these instruments by addressing the misuse of public institutions and financial systems that often facilitate transnational crime[2].

Together, these conventions provide a legal base but require reinterpretation in light of emerging technologies. The UNODC has thus emphasized "digital mainstreaming"—the integration of cyber-awareness and digital capacity into all existing treaty obligations.

FATF Recommendations

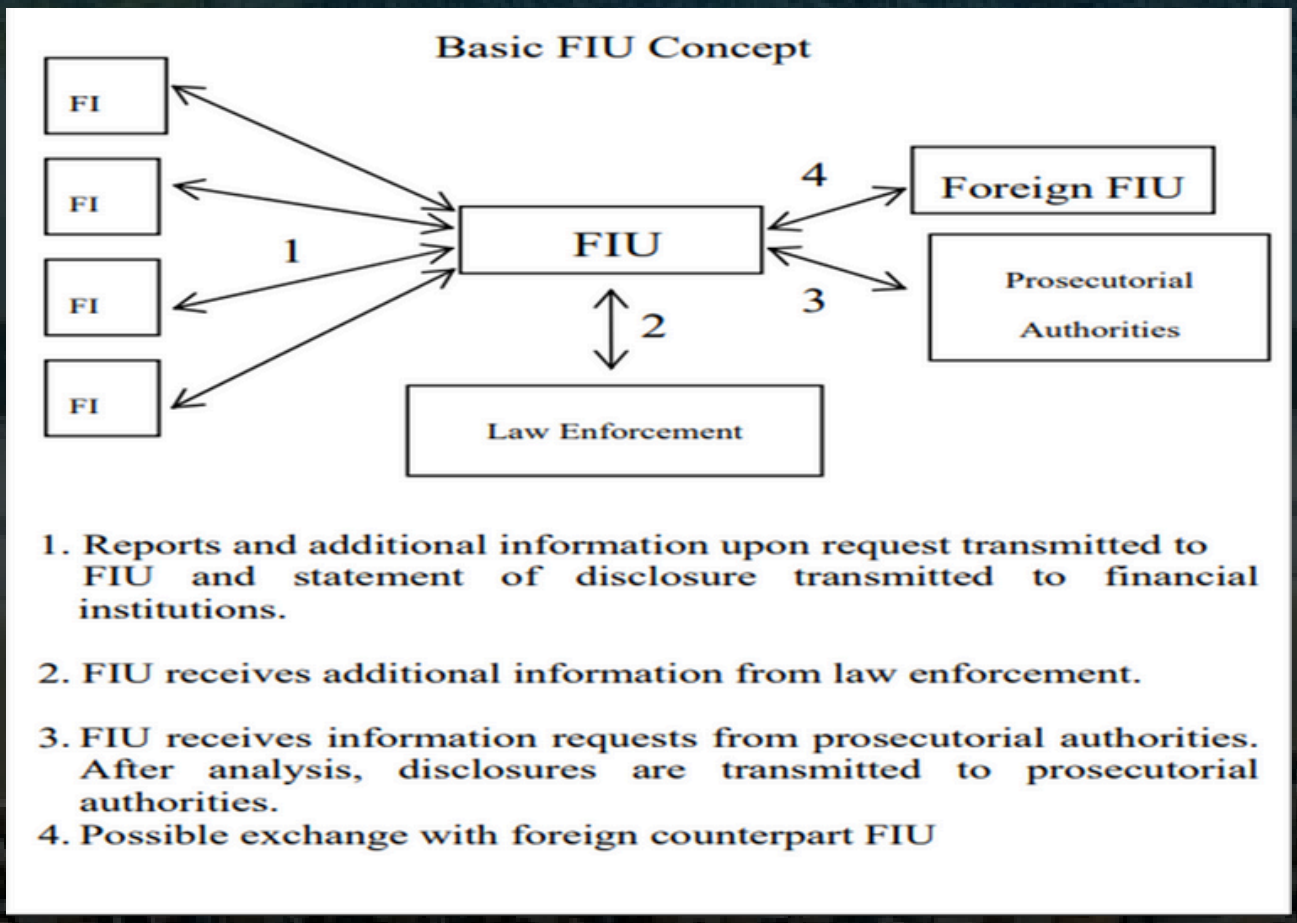
The Financial Action Task Force (FATF), established in 1989, issues globally recognized standards known as the FATF Recommendations. They require states to implement measures for anti-money laundering (AML), combating the financing of terrorism (CFT), and monitoring virtual assets[1]. In 2019, the FATF expanded its mandate to cover cryptocurrencies and digital service providers, obligating them to register, report suspicious transactions, and conduct customer due diligence[2]. While these recommendations are not legally binding, FATF uses peer evaluations and “grey-listing” to pressure non-compliant states. The FATF framework has significantly influenced national laws, yet enforcement disparities persist, particularly in low-capacity jurisdictions where digital financial systems outpace regulatory institutions.

Regional Cooperation Models

Obviously, for an issue which deems and seems to be very regional specific and requires working inter-regionally, it needs a regional approach, to say the least but that happens as Regional organizations have played an increasing role in adapting these frameworks to local contexts. The European Union's Europol and Eurojust coordinate transnational investigations across member states, integrating cyber intelligence and financial forensics[1]. The ASEAN Plan of Action to Combat Transnational Crime emphasizes digital crime and online trafficking as regional priorities[2]. The African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention) aims to create a unified approach to digital threats within Africa[3].

Such models highlight the importance of capacity-sharing and interoperability. Effective regional cooperation often acts as a bridge between local enforcement challenges and global frameworks like those of the UNODC and FATF.

The key lesson from these initiatives is that collective resilience against technologically enabled crime depends not on uniform laws, but on harmonized enforcement and continuous data exchange.



In Figure: How a Financial Intelligence Unit works

Why effective international co-operation is important

The UN has been used as a place for leaders of the countries to speak freely of their grievances since the end of World War II. It has evolved as things have changed and different types of problems have emerged. Currently we have problems of money laundering and international terrorism. A country has to identify priorities, build up its efficient domestic capacity, and determine the means for combating ML and FT taking into account its economic and environmental needs. A country's capacity building depends on its people and institutions, technological capabilities, ecological and geographical conditions and so forth. In order to strengthen international cooperation, endogenous capacity is essential and the efforts of the countries in partnership with relevant UN organizations are required to obtain endogenous capacity.

In order to construct an effective international cooperation, countries should meet three prerequisites. They are:

1. Building a comprehensive and efficient domestic capacity.
2. Ratifying and implementing the international conventions.
3. Complying with the FATF Recommendations and other sector-specific international standards.

All necessary administrative and supervisory authorities as well as an FIU with necessary powers and responsibilities should be in place adequately provided with staff, budget and other useful resources to carry out their duties efficiently, especially to oversee financial institutions. In addition, criminal justice system and judicial/prosecutorial system are two crucial factors to obtain an effective AML-CFT regime.

1)How can Member States balance the protection of individual privacy and data rights with the necessity of digital surveillance, monitoring, and intelligence-gathering for law enforcement purposes?

2)Should the regulation of cryptocurrencies and virtual assets be centralized under a global framework, or should it remain regionally adaptive under FATF and national models?

3)What frameworks can ensure accountability and legal attribution for non-state actors operating across digital platforms, including online drug vendors, crypto intermediaries, and terrorist propagandists?