

K&E MUN 2025



UNCETE

Agenda : Neutralizing Transnational Terrorist

Financing and Crypto-Enabled Extremism

A BACKGROUND GUIDE

TABLE OF CONTENTS

Letter From The Executive Board	3
Committee Overview.....	4
Keywords.....	5
How To Approach The Agenda.....	7
Agenda Overview.....	8
Past UN Initiatives.....	12
Questions A Resolution Must Answer.....	18



LETTER FROM THE EXECUTIVE BOARD

Dear Delegates,

It is with immense enthusiasm and honour that I welcome you to the United Nations Counter-Terrorism Committee (UNCTC) at KLE MUN 2025.

As members of a committee that plays a critical role in shaping international security and safeguarding global peace, you will be tasked with deliberating on one of the most pressing threats of our time: the evolution of terrorism through sophisticated financial networks and the dark corridors of crypto-enabled extremism.

In an era where extremist entities are becoming increasingly tech-savvy—harnessing decentralized digital currencies, anonymized financial platforms, and even blockchain-based ecosystems—the need for robust international frameworks and multilateral cooperation has never been more urgent.

The Executive Board urges all delegates to approach this committee with diligence, diplomacy, and an open mind. I strongly encourage you to research beyond your national policies, engage in thoughtful debate, and above all, remain respectful of the diversity of perspectives in the room.

We look forward to witnessing your leadership, your insight, and your commitment to justice and peace.

Best wishes for a stimulating and successful committee.

Warm regards,

Pranav Bhat,

Chair, United Nations Counter Terrorism Committee

COMMITTEE OVERVIEW

The United Nations Counter-Terrorism Committee (UNCTC) was established by the United Nations Security Council (UNSC) through Resolution 1373 (2001), adopted unanimously in the wake of the September 11 attacks. As a subsidiary body of the UNSC, the committee is tasked with monitoring the implementation of counter-terrorism measures, promoting international cooperation, and assisting states in developing legal and institutional capabilities to combat terrorism.

To support its mandate, the UNCTC is backed by the Counter-Terrorism Executive Directorate (CTED), established in 2004, which acts as a special political mission providing expert assessments and facilitating technical assistance to Member States.

Mandate & Key Functions

- Monitoring compliance with UNSC Resolutions related to terrorism.
- Evaluating national legislation and border controls of Member States.
- Promoting information sharing and capacity building across countries.
- Encouraging the ratification and implementation of international counter-terrorism treaties.
- Addressing emerging threats, including terrorist use of the internet, digital currencies, and foreign terrorist fighters.


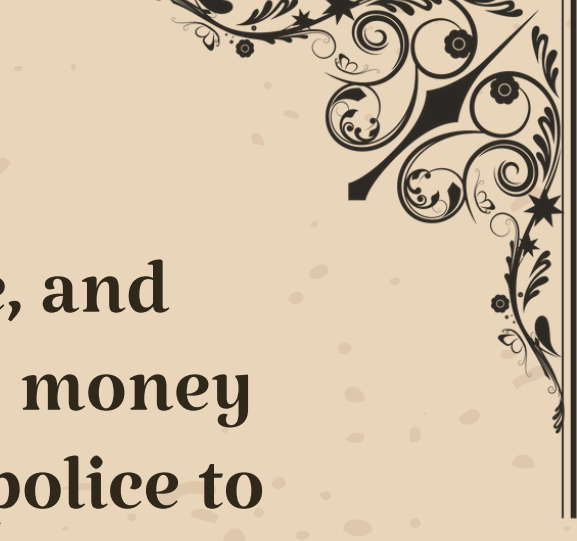
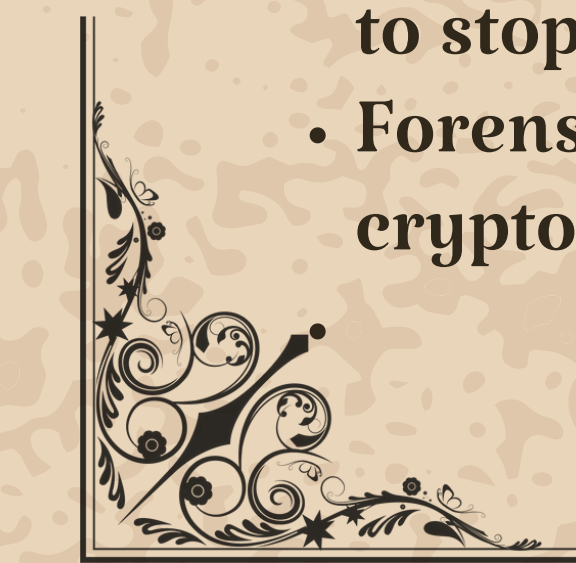

The UNCTC does not create binding international law but ensures that all Member States comply with existing obligations set by the Security Council. It plays a central role in aligning state responses to the evolving global terrorist threat landscape.



KEYWORDS



- **Terrorist Financing** – Giving money or resources to people or groups that carry out violent acts or terrorism.
- **Cryptocurrency** – A type of digital money (like Bitcoin) that is used online and isn't controlled by any bank or government.
- **Virtual Assets** – Online things that have value and can be traded or used like money (such as crypto tokens).
- **Decentralized** – Not controlled by one person or group. Instead, it runs on many computers around the world.
- **Terror Group Wallet** – A digital wallet used by terrorist groups to secretly collect, store, or move money.
- **KYC (Know Your Customer)** – A rule that makes companies check the real identity of people using their services.
- **Money Laundering** – Hiding money made from crimes and making it look like it came from a legal source.
- **Mixer / Tumbler** – A tool that hides where crypto money came from by mixing it with other people's money.
- **Privacy Coin** – Special cryptocurrencies (like Monero) that hide details about who sent or received money.
- **Blockchain** – A big digital record book that keeps track of all cryptocurrency transactions.

- 
- 
- **FIUs (Financial Intelligence Units)** – Special government agencies that collect, analyze, and share information about suspicious or illegal financial activities, especially things like money laundering and terrorist funding. They often work with banks, crypto platforms, and police to track down dirty money.
 - **International Convention for the Suppression of the Financing of Terrorism** – A global treaty that makes helping terrorists with money a serious crime.
 - **FATF (Financial Action Task Force)** – An international group that tells countries how to stop illegal money and terrorist funding.
 - **Model Law** – A sample law created by experts that countries can copy or use to make their own rules.
 - **Egmont Group** – A global network of financial investigators who share secret information about terrorist or criminal money.
 - **Sanctions** – Punishments (like freezing someone's money or banning trade) that countries use to stop bad behavior.
 - **Forensic Tool** – A high-tech software that helps track money, even if people try to hide it with crypto tricks.
- 
- 



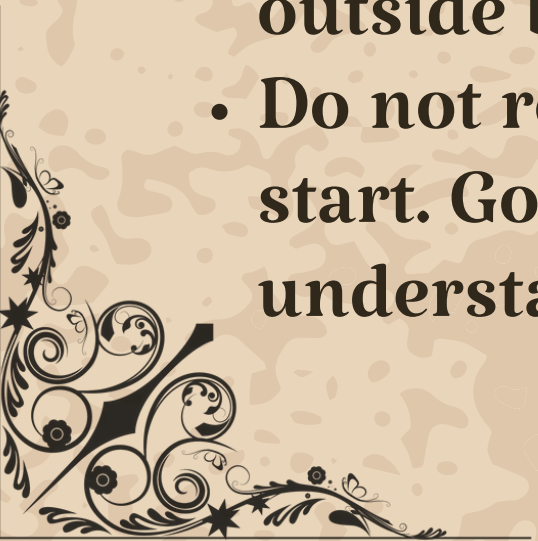

HOW TO APPROACH THE AGENDA



Dear Delegates,

Before we move on to the next section, I would like to address the following,

The agenda to be discussed is not a simple one. Cryptocurrency is a subject that is relatively new and is being studied by the entire world. Pair that with terrorism and we have something that is difficult to analyze even for the best. Hence :

- Do NOT panic if you find it difficult to understand some of the concepts discussed ahead. They are difficult, but not impossible to understand. Stay calm and read carefully.
 - There are a lot of new terms that will be introduced to you in the next few pages. Use appropriate websites to know more about them. All sources will be listed in the last page of the background guide. There is also a “Keywords” section in the previous page for your aid.
 - Try to avoid the misuse of artificial intelligence. AI tools like ChatGPT may look attractive on the outside but might not give you the most accurate information
 - Do not rely solely on the information provided in this background guide. This is a great place to start. Go through the information provided and then go deeper into the agenda for a better understanding.
- 
- 



AGENDA OVERVIEW

“Neutralizing Transnational Terrorist Financing and Crypto-Enabled Extremism”



THE RISE OF CRYPTO IN TERROR FINANCING

In recent years, terrorist organizations have increasingly turned to cryptocurrencies to fund their operations, bypass sanctions, and move money across borders discreetly. This shift from traditional cash-based methods is largely driven by the anonymity, decentralization, and speed that crypto platforms offer.

One of the most commonly exploited crypto assets is the stablecoin, particularly Tether (USDT). Unlike volatile cryptocurrencies like Bitcoin, stablecoins are pegged to fiat currencies such as the U.S. dollar, allowing extremists to maintain value and conduct cross-border transfers with minimal fluctuation. A 2024 TRM Labs report revealed that stablecoins now dominate terrorist-linked crypto transfers, with a sharp decline in Bitcoin use.

In addition, terrorist groups have started using privacy-focused cryptocurrencies such as Monero, which intentionally obscure transaction trails and wallet identities. ISKP (Islamic State Khorasan Province) has circulated online propaganda encouraging supporters to donate via Monero, making it more difficult for authorities to trace transactions.

Moreover, extremists frequently use crypto mixers, also known as “tumblers,” which combine funds from multiple sources to obscure origins. These are often paired with unhosted wallets (wallets not tied to any centralized exchange) to completely bypass know-your-customer (KYC) and anti-money laundering (AML) safeguards. A 2025 TRM analysis documented how multiple terror-affiliated wallet addresses were openly sharing tutorials on using mixers and avoiding regulatory scrutiny.

This trend reflects a troubling shift in terrorist financing strategies, underscoring the need for an urgent, harmonized global response.

REAL-WORLD INCIDENTS OF CRYPTO-ENABLED TERRORISM

ISKP-Funded Moscow Concert Attack (March 2024)

One of the most alarming events occurred in Russia when ISKP (Islamic State Khorasan Province) orchestrated a brutal attack on a concert hall near Moscow, killing over 130 civilians. Investigators traced multiple cryptocurrency wallets linked to ISKP operatives, with individual transfers ranging from \$100 to \$15,000. European nationals were involved in funding these wallets via stablecoin transactions.

Crypto Donor Arrest in Germany Ahead of Euro 2024

In June 2024, a German national was arrested for sending approximately \$1,700 in USDT to ISKP affiliates using a series of anonymized wallets and a privacy mixer. Authorities were alerted through blockchain analytics tools that flagged the wallet for suspicious activity tied to terrorism watchlists.

US DOJ and FBI Seize \$200,000 in Hamas-Linked Crypto (March 2025)

The U.S. Department of Justice seized \$200,000 in USDT across 17 crypto wallet addresses believed to be linked to Hamas-affiliated fundraising. Further investigation revealed that the network had funneled over \$1.5 million through decentralized platforms, with wallet addresses posted publicly on encrypted social channels.



First Terror Financing Conviction Using Crypto in Sweden

A landmark conviction was recorded in Sweden, where a 22-year-old was found guilty of using crypto to finance ISIS operations. The accused used small amounts of Bitcoin and Monero to bypass bank controls and contributed to overseas terror campaigns.

ISKP Wallets Traced in Central Asia (2023–2024)

Blockchain intelligence revealed that over \$2 million in USDT had been sent to pro-ISIS wallets based in Tajikistan, a hub for ISKP recruitment and propaganda. The investigation, led by Interpol and TRM Labs, led to arrests and asset freezes across Central Asia.

These incidents make it clear that cryptocurrencies have become a strategic enabler for terrorist operations, allowing them to cross borders virtually, receive micro-donations at scale, and stay ahead of outdated financial surveillance systems.



PAST UN. ACTIONS & INITIATIVES





UNSC Resolution 2462 (2019)

This landmark resolution reaffirms that all forms of terrorism financing, regardless of means, are criminal acts. It:

- **Urges Member States to criminalize direct and indirect terror financing.**
- **Broadens the legal definition to include "new and emerging technologies" like cryptocurrencies.**
- **Promotes greater public-private cooperation with financial institutions and digital platforms.**

UN Counter-Terrorism Executive Directorate (CTED) Guidance

CTED has released multiple technical reports (2021–2024) and toolkits helping member states:

- **Build blockchain surveillance capacity.**
- **Understand how privacy coins, unhosted wallets, and DeFi protocols are exploited.**
- **Train enforcement agencies to conduct digital wallet seizures and investigations.**



UNODC & INTERPOL Collaboration

The United Nations Office on Drugs and Crime (UNODC) has partnered with INTERPOL and other entities to:

- Train national FIUs (Financial Intelligence Units) on crypto-based AML/CFT frameworks.
- Provide software tools to trace on-chain transactions linked to extremist groups.
- Support field operations with blockchain forensics specialists.

Integration with FATF Guidelines

Although the Financial Action Task Force (FATF) is not a UN body, its recommendations are incorporated into UN counter-terrorism assessments. For example:

- Member States are evaluated by CTED on how well they implement FATF Recommendation 15, which directly targets virtual asset misuse.
- However, only ~20% of countries fully comply, leaving critical gaps.



CHALLENGES IN ENFORCEMENT & LEGAL LOOPHOLES



Decentralization by Design

Cryptocurrencies like Bitcoin or Monero are not controlled by any single authority, making:

- Asset seizure difficult without private keys.
- Tracking ownership nearly impossible if privacy tools are used.
- Cross-border cooperation slow due to lack of standard legal procedures.

Jurisdictional Fragmentation

Every nation treats crypto differently:

- Some (like the US or EU) have strict regulations and require KYC on all transactions.
- Others lack any laws at all, or worse, are willfully blind due to political or economic motives.
- There's no binding global convention on crypto-financing or wallet seizure.

Result: Terrorist wallets can receive funds in one country, obfuscate them in another, and cash out in a third—before law enforcement even files a request.

KEY TREATIES & LEGAL INSTRUMENTS

1. International Convention for the Suppression of the Financing of Terrorism (1999)

Most foundational treaty dealing with terrorist financing.

- **Criminalizes direct and indirect financing of terrorist acts.**
- **Requires states to seize and freeze funds used for terrorism.**
- **Used as a legal base for national anti-terror financing laws.**

2. UN Security Council Resolution 1373 (2001)

Adopted post-9/11, it's a binding resolution under Chapter VII.

- **Requires states to prevent and suppress the financing of terrorism.**
- **Calls for criminalization of terror funding, and freezing of financial assets.**
- **Establishes CTC (Counter-Terrorism Committee) to monitor compliance.**

3. UN Security Council Resolution 2462 (2019)

An important update to 1373, tailored for modern financial threats.

- **Explicitly includes new and emerging technologies (like crypto).**
- **Urges states to enhance domestic laws to cover digital assets and crowdfunding.**
- **Recommends public–private sector collaboration.**



4. Financial Action Task Force (FATF) Recommendations (especially Rec. 15)

While not a UN treaty, FATF guidelines are considered the gold standard.

- Recommendation 15 requires countries to identify, assess, and mitigate risks of virtual assets.
- Recommends “travel rule” for crypto exchanges (must collect sender and receiver info).
- Monitored by UN CTED during state compliance reviews.

Note: As of 2024, fewer than 25% of jurisdictions fully comply with Recommendation 15.

5. UNODC Model Laws & Technical Assistance Packages

The UN Office on Drugs and Crime supports member states by:

- Drafting model laws for AML/CFT (Anti-Money Laundering / Counter-Financing of Terrorism).
- Providing legal and technical guidance to align domestic laws with UN standards.
- Includes crypto and virtual asset-specific updates since 2022.

6. Egmont Group of Financial Intelligence Units (FIUs)

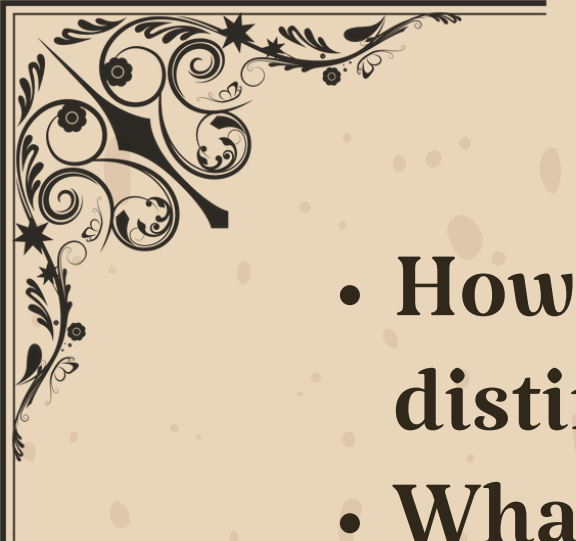

A global network of over 170 FIUs that:

- Share sensitive financial intelligence on terror finance cases.
- Act as a bridge between crypto platforms, law enforcement, and regulators.
- Though informal, it's frequently referenced in UNCTC and FATF reviews.



QUESTIONS A RESOLUTION MUST ANSWER



- 
- 
- How does the resolution define crypto-enabled terrorist financing and distinguish it from lawful use?
 - What legal frameworks or international agreements will be used or proposed to address the issue?
 - What methods will be used to trace, freeze, and recover terrorist-linked virtual assets across borders?
 - What obligations will be placed on crypto platforms, exchanges, and service providers?
 - How will the resolution support capacity-building in countries with limited technical or legal resources?
 - What mechanisms will enhance cross-border cooperation and intelligence sharing (e.g., through FIUs or the UN)?
 - How will private sector actors be engaged in detection, reporting, and compliance efforts?
 - What indicators or benchmarks will be used to assess the effectiveness of the resolution over time?