Global Classrooms®
Washington, DC
Learn. Live. Lead.

United Nations Office on Drugs and Crime

Cyber-Facilitated Financial and Organized Crime

GLOBAL CLASSROOMS DC
SPRING 2026 MODEL UN CONFERENCE

Table of Contents

INTRODUCTION TO THE COMMITTEE: UN Office on Drugs and Crime

United Office on Drugs and Crimes (UNODC), formed in 1997 in Cairo, is a global leader in the battle against crime, drugs, and terrorism. By virtue of its mandate to contribute to global peace and security, human rights, and development, UNODC has endeavored to establish robust solutions for global drug issues, organized crime, corruption and economic crime, terrorism, and criminal justice. As the magnitude of these challenges is too great for countries to tackle on their own, international networks and the committee have provided aid in implementing adjustments and measures. UNODC operates in over 80 countries with 115 field offices and 2400 staff worldwide. The agency is dedicated to assisting Member States by collaborating closely with the government and civil society to ensure the maintenance of security and justice for all. The office has also established the implementation of the 2030 Agenda for Sustainable Development and the 17 Sustainable Development Goals for its member states as a priority.The implementation supports sustainable development by emphasizing fair laws, humane justice systems, and health-focused approaches to drug use.[1]

SPRING CONFERENCE: Policy Advisors

Policy Advisors are subject-matter experts who support delegates during the conference. They do not participate in debate or voting, but they can provide guidance to help ensure your ideas and resolutions are realistic and grounded in real-world policy.

How Can You Use Policy Advisors?

Delegates are encouraged to actively consult Policy Advisors throughout the conference:

- **Opening Briefing:** Advisors will begin with a short introduction to the topic and key policy considerations.
- **Q&A Sessions:** You will have structured opportunities to ask questions about feasibility, policy context, and real-world applications.
- **During Debate:** You may submit written questions or, if allowed, yield speaking time to a Policy Advisor for a response.
- **Unmoderated Caucuses:** Advisors can help you refine ideas, identify potential allies, and strengthen draft resolutions.
- **Resolution Feedback:** Before submission, you may ask Advisors to review your proposals for clarity, feasibility, and impact.

Policy Advisors are a resource—use them to strengthen your arguments, test your ideas, and make your resolutions more effective.

STATEMENT OF THE PROBLEM

What is Cybercrime?

The proliferation of the internet has enabled unparalleled connectivity and information access on a global scale. Cybercrime is a new kind of global crime made possible by the emergence of technology. *Cybercrime, unlike other kinds of crime, is not restricted by geographical boundaries, allowing cybercriminals to commit large-scale crimes fast and easily.*[2] The United Nations defines cybercrime as "an act that violates the law that is committed using information and communication technology (ICT) to either target networks, systems, data, websites, and/or technology in order

[1] United Nations Office on Drugs and Crime, *About UNODC*, United Nations, https://www.unodc.org/unodc/en/about-unodc/index.html.

[2] United Nations Office on Drugs and Crime, *UNODC – Cybercrime*, United Nations, https://www.unodc.org/unodc/en/cybercrime/index.html.

to support a crime."[3] The **origins of global cybercrime** may be traced back to the 1980s, when the internet and computer networks began to proliferate. In the early days of cybercrime, most of the perpetrators were solitary people who exploited computer system weaknesses for personal benefit. As the Internet and computer networks expanded, however, so did the skill of cybercriminals. Criminal groups have begun to commit cybercrimes to steal sensitive data, destroy key infrastructure, and conduct espionage.[4]

The Internet was born on January 1, 1983, when the **Advanced Research Projects Agency Network (ARPANET)**, the first public packet-switched computer network, adopted the **Internet Protocol Suite (TCP/IP)**, a standard communications protocol. Since then, the number of internet users has risen annually[5]; presently, over 5 billion people have access to the internet. To comprehend the impact of cybercrime on the world today, one must first comprehend the evolution of contemporary technology over the past few decades, the cause for cybercrime's pervasive nature, and what governments and businesses have done to strengthen cybersecurity. Cybercrime is freely accessible and has the potential to be far more harmful than traditional types of crime. Internet anonymity and accessibility contribute significantly to cybercrime's appeal. Cybercriminals may easily conduct crimes while remaining concealed. When a user joins a virtual private network (VPN), their IP address is swapped with that of the VPN operator. Similarly, proxy servers conceal a computer's real IP address. The program Tor, which stands for "The Onion Router," enables users to visit websites and communicate anonymously over the internet.[6] By utilizing these tools, criminals can conceal their identity while committing various crimes, **including moving illicit funds across borders and operating dark web marketplaces for fraud.**

Cyber-enabled/facilitated Crime:

There are two primary types of cybercrime: cyber-dependent and cyber-enabled/facilitated[7].[8] **Cyber-dependent** (or sometimes referred to as "pure cyber-crimes") are crimes that can only be committed using ICT.[9] **Cyber-enabled (or also referred as cyber-facilitated)** crimes are traditional crimes such as fraud, identity theft, or money laundering[10] that can now be committed on a larger scale and at greater speed due to technological advancements.[11]

UNODC is particularly concerned about the growing overlap between cybercrime and financial crime, including online fraud, money laundering via digital assets, and the use of digital platforms by transnational organized crime groups to expand their operations worldwide. Unlike traditional financial crime, it operates across borders at unprecedented scale and speed, making detection and prosecution deeply challenging. According to UNODC reports, groups exploiting ICT for scams, money laundering, and/or fraud are generating massive amounts of profit, even equivalent to "15% of the global GDP."[12] **The FBI's Internet Crime Complaint Center (IC3) received 859,532 complaints of suspected internet crime in 2024, with reported losses exceeding $16 billion, a 33% increase from the prior year.**[13] Cyber-facilitated

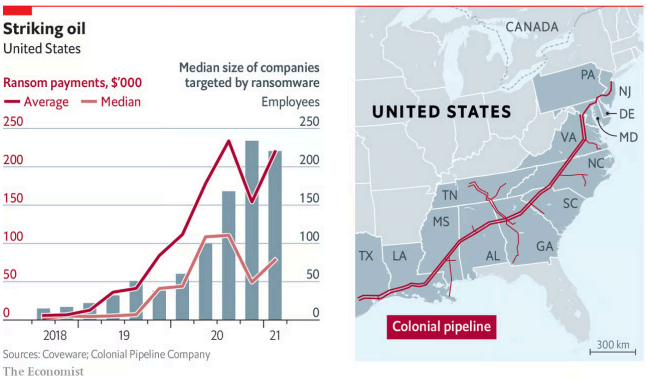
---

[3] Ibid.
[4] Center for Strategic and International Studies (CSIS), *Cybercrime and Cybersecurity: A Global Reality Check*, 2022, https://www.csis.org/analysis/cybercrime-and-cybersecurity-global-reality-check.
[5] Statista, *Worldwide Digital Population, April 2022*, July 26, 2022, https://www.statista.com/statistics/617136/digital-population-worldwide/.
[6] Dan Rafter, *Proxy vs. VPN: 4 Differences You Should Know*, Norton, https://us.norton.com/internetsecurity-privacy-proxy-vs-vpn.html.
[7] The terms "cyber-enabled" and "cyber-facilitated" are often used interchangeably in international frameworks, including by UNODC, to describe crimes where technology serves as the vehicle for financial gain or organized criminal activity. This committee uses both terms in that sense.
[8] Europol, *Internet Organised Crime Threat Assessment 2021*, 2021, https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-2021.
[9] Home Office, *Review of the Handling of Cases of Complex and Organised Crime, Chapter 1*, United Kingdom, 2017, https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf.
[10] Definition: **Money laundering** is the process of disguising illegally obtained money so it appears to come from a legitimate source.
[11] Home Office, *Review of the Handling of Cases of Complex and Organised Crime, Chapter 1*, United Kingdom, 2017, https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf.
[12] United Nations Office on Drugs and Crime (UNODC), *Cyber Organized Crime Activities*, Education for Justice (E4J) Cybercrime Module 13, https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html.
[13] Federal Bureau of Investigation, *FBI Releases Annual Internet Crime Report*, April 23, 2025, https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report.

financial and organized crime is a global problem that requires countries to work together. This guide looks at the major forms of these types of crime, the groups behind them, and current international frameworks in place to address them. **Delegates should identify gaps in these rules and suggest ways to help countries better prevent, investigate, and prosecute such crimes.**

KEY TRENDS:

[14]**1. Professionalization of Fraud Operations**: According to the Global Anti-Scam Alliance (GASA), fraud networks now operate like well-oiled multinational corporate machines, owing to developments in modern technology. These types of operations have proliferated across the Southeast Asia region, and transnational organized crime networks are linked to underground money laundering, which has now become ubiquitous in the area. For example, **more than 400 of these organization**s are operating in the Philippines alone. UNODC regional analyst, John Wojcik said, "*Cyber-enabled fraud perpetrated by powerful transnational criminal networks has evolved into a thriving multi-billion-dollar illicit industry that now exceeds the GDP of several countries in Southeast Asia combined*."[15] Platforms such as telegram have offered data harvesting[16], malware-as-a-service[17], and AI-fraud tools. One example of how these activities are carried out is Ransomware-as-a-Service (RaaS); developers create harmful software and lease it to criminal organizations. RaaS has an intricate business model, with subscription models and help desks for users. Some operators offer tiered pricing plans depending on the level of tools and services included, while others take a percentage of the ransom as payment. This structure makes cybercrime more accessible, even to actors with limited technical skills.



The **2021 Colonial Pipeline** attack is one example of a RaaS-based operation; the largest refined oil products pipeline in the United States was subject to a cyberattack that disrupted fuel supplies across the east coast. In May 2021, a Russian-based RaaS agency, The Dark Side group's affiliate gained access to the Pipeline's VPN (partially due to a lack of multi-factor authentication) and deployed the network with Ransomware. DarkSide operated like a criminal enterprise with a core development team, affiliate network, profit-sharing system, and even user support functions that resembled a legitimate software company. Affiliates licensed the ransomware, carried out attacks independently, and sent a cut of the ransom back to the core group. The Colonial Pipeline attack itself was executed by an affiliate rather than the core team, highlighting a structured division of labor between developers, operators, and affiliates.

Ransomware encrypts[18] critical data and restricts users from accessing the system until a ransom is paid. The attack affected key operational systems, including accounting and billing. To prevent the spread of ransomware, Colonial Pipeline shut down its operations from May 7-12, temporarily halting fuel supplies across its pipeline network. This decision led to fuel shortages, panic buying, and price increases across the South and East Coast, with several gas stations running out of fuel. The shutdown also disrupted air travel. In response, President Biden declared a state of emergency, and state officials such as Georgia's governor also issued emergency measures, including temporary fuel tax adjustments. Operations resumed on May 15th, the company paid 75 bitcoin[19] as ransom, some of which was later recovered by the

---

[14] *The Economist*, "Ransomware attacks like the one that hit Colonial Pipeline are increasingly common," *The Economist (graphic detail)*, May 10, 2021, https://www.economist.com/graphic-detail/2021/05/10/ransomware-attacks-like-the-one-that-hit-colonial-pipeline-are-increasingly-common.

[15] UNODC, *Cyberfraud Syndicates Observed Deploying New Tech*, 2024, https://www.unodc.org/roseap/en/2024/08/cyberfraud-syndicates-analyst-meeting/story.html.

[16] Definition: Data harvesting is the automated collection of large amounts of personal or online data, often without users' consent.

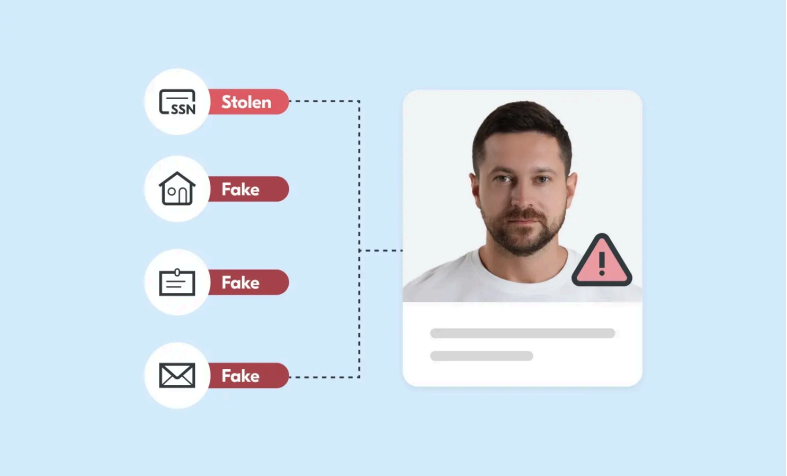
[17] Definition: **Malware-as-a-service (MaaS)** is a cybercrime business model where attackers sell or rent ready-made malware to others, allowing even non-technical users to launch cyberattacks.

[18] Definition: **Encrypt** means to convert information or data into a coded form so that only authorized parties can read it.

[19] Definition: **Bitcoin** is a decentralized digital currency that allows people to send and receive money electronically without the need for a bank or central authority.

DOJ. This incident demonstrates how cyber-facilitated crime can disrupt critical supply chains and generate significant economic instability.[20]

2. Generative AI[21]**:** The rapid expansion of generative AI has led to cybercriminals using AI & deepfakes[22] to commit crimes with ease. AI-related scams have increased by 1210% in 2025 [23]; some studies project losses up to $40 billion by 2027.[24] AI is being utilized to enhance and automate **phishing** emails, which are fraudulent messages designed to trick individuals into revealing sensitive information such as passwords or financial details. An example of a highly personalized and targeted phishing scam is **Business Email Compromise (BEC). BEC refers to the impersonation of executives or senior management** to generate fake emails to trick employees into transferring unauthorized money or sharing sensitive information.



While Business Email Compromise typically relies on email-based impersonation, similar fraud schemes are now emerging using AI-generated audio and video to create even more convincing deceptions. For example, an employee in a Hong Kong-based financial firm made an **unauthorized payment of $25 million** to the fraud agency following an AI-generated conference call with his boss and colleagues. Upon investigating the incident, superintendent Baron Chan Shun-ching described, "(In the) multi-person video conference, it turns out that everyone [he saw] was fake."[25] This fraud-scheme combines deepfakes and voice-cloning; AI tools can clone a voice using as little as three seconds of clear audio. In addition to fraudulent transfers, AI is also being leveraged to bypass Know-Your-Customer[26] checks on financial platforms; this is termed as **Synthetic Identity Fraud**. Unlike traditional identity fraud, synthetic identity fraud does not involve impersonating a real person. Instead, it involves creating a fabricated identity designed to pass verification checks. These identities may combine real information, such as a valid Social Security number, with fictitious details like a name or address, and may also leverage AI tools to generate deepfakes or other convincing digital artifacts. Although synthetic identity fraud predates the rise of artificial intelligence, advances in AI have significantly increased **its scale and sophistication**, enabling criminal networks to create more realistic identities and bypass verification systems with greater ease. The aforementioned are two examples of how AI is being used to commit and **automate** traditional financial fraud. However, note that generative AI is rapidly evolving and is being used in many different aspects of cyber-enabled crime.

---

[20] INSURICA, *Cyber Case Study: Colonial Pipeline Ransomware Attack*, 2024, https://insurica.com/blog/colonial-pipeline-ransomware-attack/.

[21] Definition: **(i) Artificial Intelligence (AI)** refers to the field of computer science focused on creating systems or machines that can perform tasks that typically require human intelligence. These tasks include learning from data, recognizing patterns, understanding language, making decisions, and solving problems.
(ii) Generative AI is a type of artificial intelligence that goes beyond analyzing or classifying data and instead creates new content, such as text, images, audio, or video.

[22] Definition: **Deepfakes** are synthetic media—usually videos, images, or audio—created using artificial intelligence to realistically replace a person's likeness or voice with someone else's. They are generated using machine learning techniques, especially deep neural networks, and can make it appear as though someone said or did something they never actually did.

[23] Vectra AI, *AI Scams Explained: How AI-Powered Fraud Works and How Enterprises Detect It*, 2026, https://www.vectra.ai/topics/ai-scams.

[24] Vectra AI, *AI Scams Explained: How AI-Powered Fraud Works and How Enterprises Detect It*, 2026, https://www.vectra.ai/topics/ai-scams.

[25] INSURICA, *Cyber Case Study: Colonial Pipeline Ransomware Attack*, 2024, https://insurica.com/blog/colonial-pipeline-ransomware-attack/.

[26] Definition: A **Know Your Customer (KYC)** check is a mandatory verification process used by financial institutions and businesses to confirm a customer's identity, reduce fraud, and prevent illegal activities like money laundering.

3. **Exploitation of Cryptocurrency: Cryptocurrency** is a form of digital currency[27] that exists only electronically and is not issued or controlled by a central authority such as a government or bank. It operates on decentralized networks, typically using blockchain technology to record and verify transactions.[28] The decentralized nature of cryptocurrency makes it conducive for financial crimes. One such example is a "Pig-butchering" scam where scammers use a fabricated identity to catfish[29] victims often through social media platforms, building trust and intimacy to manipulate them into investing in fraudulent platforms. Victims are provided guidance on converting their cash into cryptocurrency through a publicly available service and are then asked to transfer the funds to a fake platform promising "*huge returns*." The platforms are designed to look like legitimate trading platforms and may initially even display high returns, but once the funds are transferred, it is difficult to ever recover the funds.In a devastating example of a pig-butchering scam, an 82-year-old man from Northern Virginia died by suicide in 2024 after transferring all of his life savings to an online scammer he met on Facebook.[30] Other cyber-enabled crypto-based crimes include fake investment schemes, ransomware payments demanded in digital currency, phishing attacks targeting crypto wallets, fake **initial coin offerings (ICOs) (*fundraising schemes* where scammers raise money for a non-existent or misleading crypto project and then disappear with investors' funds)**, **rug pulls (a crypto scam where developers suddenly take investors' money and abandon the project, leaving the currency worthless)**, and the use of cryptocurrency to facilitate money laundering[31].

Laws surrounding the fraudulent transfer of digital funds vary by region and continue to evolve, particularly as regulators work to address the emerging risks associated with crypto-based financial crime.[32] The European Union's Markets in **Crypto-Assets (MiCA)** regulation is one prominent example aiming to curb crypto-based financial crimes; it standardizes and institutionalizes a common set of rules and regulations for all crypto-based transactions. It establishes licensing requirements for all crypto-asset providers (CASPs).[33] Other advanced economies such as the United Kingdom and India have expanded their anti-money laundering laws to cover virtual assets, while the United States has created a Virtual Asset Exploitation unit within the FBI to assess and combat crypto-based crimes. However, the absence of global standards emphasizes the need for a coordinated multilateral-level response that this committee is called upon to address.

4. Cyber-Facilitated Crime and Human Trafficking: One of the most alarming developments in recent years is the **intersection of cyber-facilitated financial crime and human trafficking**. Flagright, an AI-operating system for financial crime compliance, describes "*human trafficking as both a human rights violation and a financial crime.*" According to ILO estimates, forced labor generates around $236 billion in profits every year. Human traffickers are using cyber-technology to expand their operations and increase revenue.[34] ICT is employed at various stages of a human trafficking operation: in the initial stages, social media (or similar) platforms may be used to lure and track victims, and

---

[27] Definition: **Digital currency** is any form of money that exists exclusively in electronic or digital form, with no physical counterpart like paper bills or coins. It is stored in digital wallets, transferred over computer networks, and allows for instantaneous, often lower-cost, peer-to-peer transactions without intermediaries.

[28] Ibid.

[29] Definition: **Catfish (or "catfishing")** is when someone creates a fake identity online to deceive others, usually by pretending to be someone else in order to build a relationship, gain trust, or manipulate them emotionally or financially.

[30] *CNN*, *Killed by a Scam: A Father Took His Life After Losing His Savings to International Criminal Gangs*, June 17, 2024, https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk.

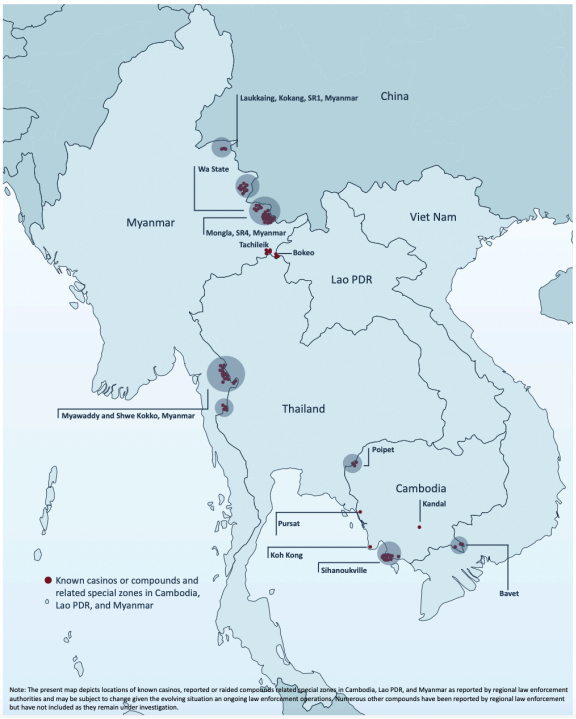
[31] Definition: **Money laundering** is the process of making illegally obtained money appear legal by hiding its criminal origin. In the context of **cryptocurrency**, it involves using digital currencies and blockchain transactions to move or disguise illegal funds, making them harder for authorities to trace and link back to criminal activity.

[32] Ibid.

[33] Coinbase, *What Is MiCA (Markets in Crypto-Assets Regulation)?*, 2025, https://www.coinbase.com/learn/your-crypto/what-is-mica-markets-in-crypto-assets-regulation. (coinbase.com)

[34] International Labour Organization, *Annual Profits from Forced Labour Amount to US$236 Billion, ILO Report Finds*, March 19, 2024, https://www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds.

once a victim is recruited, location tracking and similar technologies can be used to maintain control and prevent escape.[35]



According to UNODC reports, these victims are trafficked for forced criminality, meaning they are forced to commit crimes including cyber-enabled offenses. Specifically, the **Southeast Asia region** has seen highly organized criminal syndicates leveraging **Special Economic Zones (SEZs)**[36] and unemployment to enable their operations. The image on the left maps out casino and scam centers in Cambodia, Lao PDR, and Myanmar.[37] Laws in the region are insufficient and enforcement is weak. Human rights groups indicate that public officials in both Myanmar and Cambodia are directly profiting from these criminal operations, with Myanmar's military leasing land to scam compounds and high-level Cambodian officials linked to criminal networks laundering billions in proceeds.

Additionally, digital currencies have enabled the transfer of illegal funds with ease. Due to their electronic and decentralized nature, digital currencies have changed traditional patterns of money laundering; illegally obtained funds still need to be concealed, but criminals may use different methods that are often harder to trace. Digital funds can be transferred across borders with ease and also provide a degree of anonymity. Traditional money laundering has become increasingly difficult due to strict anti-money laundering laws.[38]

UN & INTERNATIONAL ACTION: [39]

Over the years, several legal frameworks have emerged to address cyber-facilitated financial and organized crime, though gaps remain. The **United Nations Convention against Transnational Organized Crime (UNTOC)**, adopted in 2000, is the primary international instrument against transnational organized crime, requiring states to criminalize money laundering, participation in organized criminal groups, and corruption, and to adopt frameworks for extradition and mutual legal assistance.[40] The Council of Europe's Budapest Convention on Cybercrime, ratified by 65 countries, provides a complementary framework for international cooperation in investigating and prosecuting **cybercrime**.[41] Most recently, the **United Nations Convention against Cybercrime**, known as the **Hanoi Convention**, was adopted by consensus through General Assembly Resolution 79/243 on December 24, 2024, marking the first international anti-crime treaty in over 20 years, with 72 signatories following its

---

[35] United Nations Office on Drugs and Crime, *Technology Facilitating Trafficking in Persons*, *E4J University Module Series: Trafficking in Persons & Smuggling of Migrants (Module 14)*, 2019, https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.html.

[36] Definition: **Special Economic Zones (SEZs)** are designated, often fenced-in, geographical areas within a country that operate under distinct, more liberal economic laws, regulations, and tax policies compared to the rest of the nation. These zones are designed to attract and boost foreign investment.

[37] United Nations Office on Drugs and Crime, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia: Policy Brief – Summary Overview*, August 2023, https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Summary_Policy_Brief.pdf.

[38] *Examples of national anti-money laundering laws include the U.S. Bank Secrecy Act (1970), the UK Proceeds of Crime Act (2002), India's Prevention of Money Laundering Act (2002), and China's Anti-Money Laundering Law (2006).*

[39] International Model United Nations Association, *UNTOC: United Nations Convention Against Transnational Organized Crime (NHSMUN Committee Page)*, accessed 2026, https://www.imuna.org/nhsmun/nyc/committees/untoc-convention-against-transnational-organized-crime/;

[40] United Nations Office on Drugs and Crime, *United Nations Convention against Transnational Organized Crime (UNTOC) – Introductory Overview*, accessed 2026, https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

[41] United Nations Children's Fund (*UNICEF*), *Who We Are*, accessed 2026, https://www.unicef.org/who-we-are.

signing ceremony in Hanoi, Vietnam in October 2025.[42] On the financial crime side, the **Financial Action Task Force (FATF),** an intergovernmental organization, sets global anti-money laundering standards and since 2018 has extended those standards to virtual assets.[43] At the regional and national level, responses have been uneven. The EU's Markets in Crypto-Assets regulation, enacted in December 2024, represents a landmark framework for virtual assets currently in force.[44]

Questions to Consider:

1. What cyber-facilitated financial crimes pose the greatest threat to your country's economy and citizens, and what measures has your government taken to address them?
2. How does your country regulate cryptocurrency exchanges and virtual asset service providers, and what gaps exist in your current legal framework?
3. Is your country compliant with FATF standards on virtual assets? If not, what obstacles prevent full compliance?
4. How does your country's Financial Intelligence Unit coordinate with international partners to track and disrupt illicit financial flows?
5. What role should the United Nations play in setting enforceable global standards for cyber-facilitated financial crime, given the limitations of existing frameworks like the Hanoi Convention?
6. How should the international community address the overlap between cyber-facilitated financial crime and human trafficking, particularly in regions where state actors are complicit in criminal operations?
7. What responsibilities do private sector actors (including cryptocurrency exchanges, and financial institutions) bear in preventing cyber-facilitated financial crime?
8. Should states bear responsibility when cyber-facilitated financial crime originates within their borders but targets victims abroad?
9. How should the international community respond when national governments are complicit in or profit from cyber-facilitated organized crime?

Glossary:

Money laundering is the process of disguising illegally obtained money so it appears to come from a legitimate source.
Data harvesting is the automated collection of large amounts of personal or online data, often without users' consent.
Malware-as-a-service (MaaS) is a cybercrime business model where attackers sell or rent ready-made malware to others, allowing even non-technical users to launch cyberattacks.
Bitcoin is a decentralized digital currency that allows people to send and receive money electronically without the need for a bank or central authority.
Artificial Intelligence (AI) refers to the field of computer science focused on creating systems or machines that can perform tasks that typically require human intelligence. These tasks include learning from data, recognizing patterns, understanding language, making decisions, and solving problems.
Generative AI is a type of artificial intelligence that goes beyond analyzing or classifying data and instead creates new content, such as text, images, audio, or video.
Deepfakes are synthetic media—usually videos, images, or audio—created using artificial intelligence to realistically replace a person's likeness or voice with someone else's. They are generated using machine learning techniques, especially deep neural networks, and can make it appear as though someone said or did something they never actually did.

---

[42] United Nations Office on Drugs and Crime, *United Nations Convention against Cybercrime: Strengthening International Cooperation to Combat Crimes Committed Through ICT Systems*, accessed 2026, https://www.unodc.org/unodc/en/cybercrime/convention/home.html.
[43] Financial Action Task Force, *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, July 9, 2024, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html.
[44] Legal Nodes, *The EU Markets in Crypto-Assets (MiCA) Regulation Explained*, November 11, 2025, https://www.legalnodes.com/article/mica-regulation-explained.

A **Know Your Customer (KYC)** check is a mandatory verification process used by financial institutions and businesses to confirm a customer's identity, reduce fraud, and prevent illegal activities like money laundering.
Digital currency is any form of money that exists exclusively in electronic or digital form, with no physical counterpart like paper bills or coins. It is stored in digital wallets, transferred over computer networks, and allows for instantaneous, often lower-cost, peer-to-peer transactions without intermediaries.
Catfish (or "catfishing") is when someone creates a fake identity online to deceive others, usually by pretending to be someone else in order to build a relationship, gain trust, or manipulate them emotionally or financially.
Money laundering is the process of making illegally obtained money appear legal by hiding its criminal origin. In the context of **cryptocurrency**, it involves using digital currencies and blockchain transactions to move or disguise illegal funds, making them harder for authorities to trace and link back to criminal activity.
Special Economic Zones (SEZs) are designated, often fenced-in, geographical areas within a country that operate under distinct, more liberal economic laws, regulations, and tax policies compared to the rest of the nation. These zones are designed to attract and boost foreign investment.

Position Paper Guidelines:

In order to be eligible for a committee award, delegations must submit one (1) position paper per country (i.e. if two delegates are representing the United States, they will only submit one position paper between the two of them).

What is a Position Paper?
A position paper is a short document that outlines a country's opinion on an issue. The paper includes a short summary of what the issue or problem is, explains why the country is interested in the issue, and communicates the country's stance on what should be done to address the issue. A position paper is written as if you were the actual representative of the country stating its position. Your personal opinions on the issue should not be included. A position paper is not a summary of your country's GDP, government, economy, languages, etc. unless directly relevant to the issue. Only one position paper is written per country, per grade school committee; **if there are 2 or 3 delegates representing the same country on a committee, they should write the paper together**.

Why write a Position Paper?
Writing a position paper will help you organize why an issue matters to your country and what your country wants done on the issue. The first thing you will likely do in committee is present an opening speech about your country's position. You should be able to pull portions of a well written position paper into an introductory speech on your country's perspective.

How to Write a Position Paper

(1) Research the Issue. The questions you want to answer are:
- How does this issue affect your country?
- How does this issue affect your country's neighbors or allies?
- Is this a global problem that impacts everyone?
- What would your country like to see done on this issue?
- Are there countries or groups of people who will be particularly sensitive to addressing this issue?
- Are there any conventions or resolutions on the topics that your country has signed or ratified?
- What are UN actions on the issue? Has your country supported or opposed these actions?
- Keep in Mind: What a country says, and what it actually believes should be done may be different. Also, some countries may believe that no action should be taken on an issue. They may disagree with how others feel or may not want international involvement. It is okay if your position is that the international community should do nothing, but you will need to explain why.

(2) Brainstorm Specific Actions. Come up with 3-4 specific things that can be done to reach the outcome your country desires. For example: "The United States believes we should send a peacekeeping mission to monitor human rights abuses in Syria and encourage talks between both sides." You will present these ideas in committee as possible solutions to the problem and attempt to pass a resolution which includes these actions.

(3) Outline Your Paper. Make an outline of what points you want to cover in your paper and the order in which

you would like to address them. Remember a good paper should briefly explain the problem, explain why your country cares about the issue, and inform others what your country should like to see done. If you know other countries favor a solution that you will disagree with, make sure to include why your country disagrees.

(4) Write your Paper. Position papers should be written from the perspective of the country you are representing. Rather than being a report on the topic, a position paper should explain what your country wants to see done to address the issue. Start by giving a brief summary of the issue and how it impacts your country. Then explain the specific actions you would like to see taken. Close by summarizing your country's overall position. Proper grammar and spelling are a must.

Award Criteria and Eligibility

- The ideal position paper will have a clearly defined and summarized topic with your country's position clearly outlined. Points are also awarded for organization, style and correct grammar.
- GCDC Staff will be fact checking position papers, so be sure to include the most up to date information and a bibliography (if using in text citations, a Works Cited page MUST be included)
    - Proper source citation: if an idea or quote came from another source, you must provide a footnote / citation.
- Papers will be disqualified if the conference staff has discovered that students did not write their own papers or that content has been plagiarized.
- **Make sure your position paper must have the required header below! Do not create any additional title pages - points will be deducted for improper format.**
- **Formatting Requirements: 500 words minimum, 1,500 words maximum. Times New Roman font, 12- point size**

Required Position Paper Header

Committee:
Country:
Topic:
School:
Delegate Name(s)