



TroyMUN'26

UNODC

Combating the Rise of Cyber-Enabled
Transnational Organised Crime and
Darknet Marketplaces

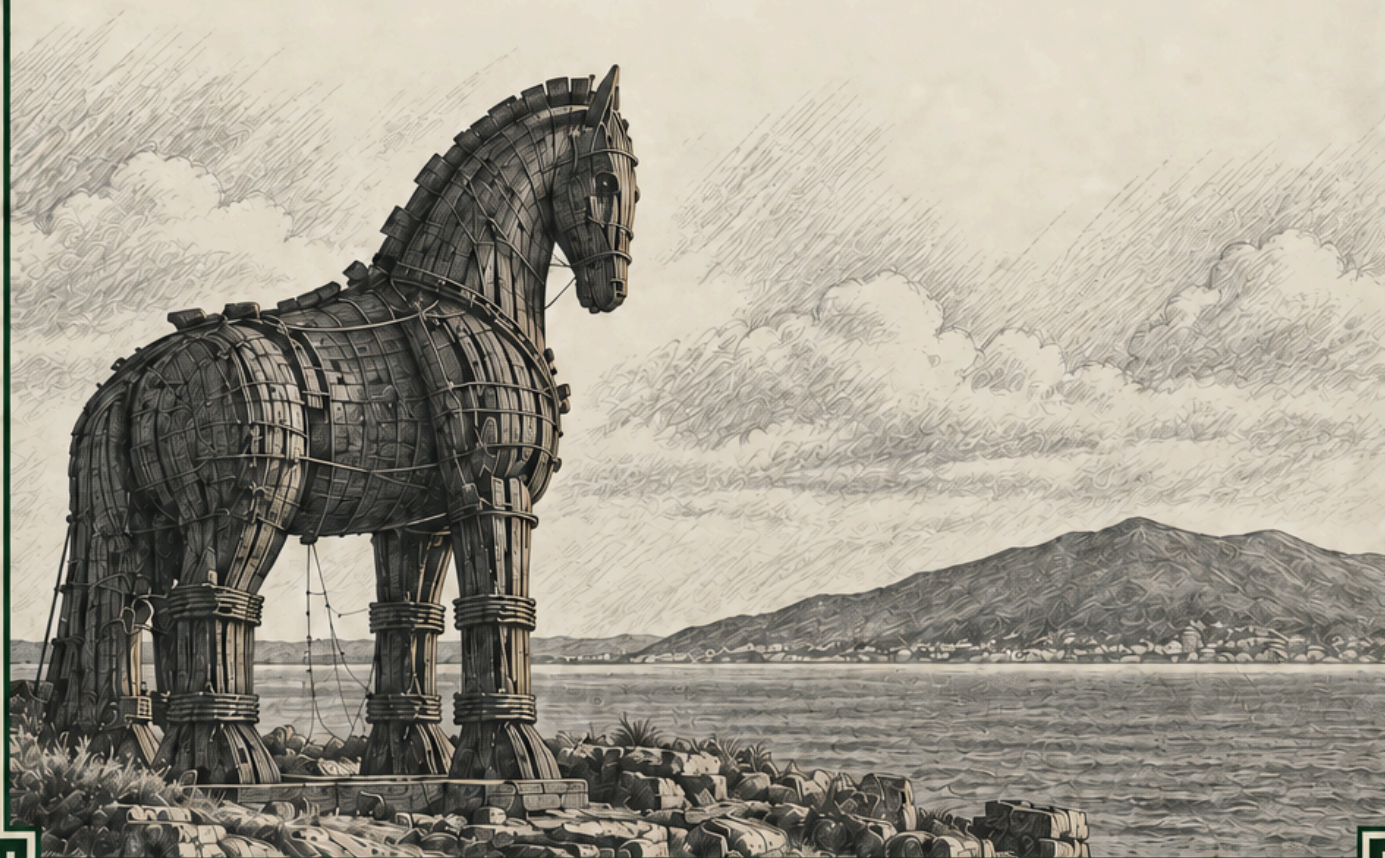


TABLE OF CONTENTS

- I. Letter from Secretary-General**
- II. Letter from Mentor Under-Secretary-General**
- III. Letter from Under-Secretary-General**
- IV. Introduction to the Committee: United Nations Office on Drugs and Crime**
- V. Introduction to the Agenda Item: Combating the Rise of Cyber-Enabled Transnational Organised Crime and Darknet Marketplaces**
 - A. Overview of the Agenda**
 - B. Historical Background of the Agenda Item**
 - 1. The Evolution of Organized Crime**
 - 2. The Rise of Cybercrime**
 - 3. The Emergence of Darknet Marketplaces**
 - 4. International Response**
 - C. Sustainable Development Goals**
 - 1. SDG 16**
 - 2. SDG 17**
 - 3. SDG 8**
 - D. Understanding Cyber-Enabled Organized Crime and Darknet Marketplaces**
 - 1. Cyber-Enabled vs Cyber-Dependent Crime**
 - 2. Characteristics of Cyber-Enabled Organized Crime**
 - 3. How Darknet Marketplaces Operate**
 - 4. Common Criminal Activities**
 - 5. Why Darknet Marketplaces are Difficult to Combat**

E. Current Challenges

- 1. Ransomware**
- 2. Cryptocurrency-based Money Laundering**
- 3. AI-Assisted Cybercrime**
- 4. Cross-Border Investigations**
- 5. Data Sharing and Digital Evidence**
- 6. Public-Private Cooperation**

F. Existing International Frameworks

- 1. United Nations Convention against Transnational Organized Crime (Palermo Convention)**
- 2. Budapest Convention on Cybercrime**
- 3. INTERPOL & Europol Operations**
- 4. UNODC Global Programme on Cybercrime**
- 5. FATF Standards on Virtual Assets**
- 6. Regional Cooperation Mechanisms**

G. Emerging Trends

- 1. AI-powered Criminal Activities**
- 2. Ransomware-as-a-Service (RaaS)**
- 3. Decentralized Darknet Marketplaces**
- 4. Privacy Coins and Cryptocurrency Mixers**
- 5. Future Challenges for International Law Enforcement**

VI. Case Studies

VII. Questions to Ponder

VIII. Further Reading

IX. Bibliography

I. Letter from Secretary-General

Esteemed Prospective Participants,

On behalf of TROYMUN Family, I would like to welcome you all to the ninth edition of TROY Model United Nations Conference. My name is Baran Akarsu and it is an utmost honor and privilege to serve as the Secretary-General of TROYMUN 2026. The ninth edition of TROYMUN will be held with the collaboration of Parion Hotel and Çanakkale College once again and it will take place in Çanakkale. While the junior edition of TROYMUN will take place between 23th-25th of November, the senior edition will be held between 27th and 29th of November. Since our last edition We are extremely delighted and excited to meet once again and discuss some of the world's current problems. This year, we will host five committees in each of our editions. The committees will be a bit more interesting, more related to our current life and new rather than our past editions. The topic of Ensuring Habitat Protection and Biodiversity Conservation will be discussed in United Nations Environmental Programme for our Junior Edition. Reminding that it will be the first time of hosting UNCoST, The discussion is going to be covered under Raising Awareness on Usage of AI and Combatting the Misuse of Artificial Intelligence for our Junior Edition. UNICEF with the topic of The Effects of Social Media Usage and Digital Bullying on Children's Mental Health: International Maritime Organization with the issue of Protecting Oceans from Plastic Pollution and Maritime Waste for our Junior Edition. Not to forget our last and another new gen committee for Junior Edition, include an exciting wait for you to shine as a star. FCC: The Galactic Senate In the Futuristic Crisis Committee, delegates will prepare for the upcoming galactic elections with their factions. There will be four factions competing in the elections.

Besides the elections, delegates will also cooperate with each other to solve the problems of the galaxy. Meanwhile for our Senior Edition,

United Nations Office on Drugs and Crime will discuss Combating the Rise of Cyber-Enabled Transnational Organized Crime and Darknet Marketplaces. UNWomen with the topic of Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention). Senior Edition Of UNICEF's Agenda Item will be Ensuring the Protection of Children's Rights in Armed Conflicts: The Case of Gaza. As you knew from our last edition, We gathered together in a committee to dream about the America. We know it is in your dreams before your sleeps, American Dreams! An exciting rehandling of Historical U.S Senate comes with a new discussion; The Civil Rights. Our last and fifth for our Senior Edition will be a Crisis Committee. JCC will be with us in order to discuss The Napoleonic Era. We are looking forward to see you as a star, a delegate, a diplomat in our ninth edition which is special and the last before the double digits.

Delighted to hear your solutions on these crucial topics and wish you fruitful debates. A group of experienced MUN delegates as well as successful and exemplary individuals well versed in the topics at hand will chair and monitor our committees. I have full faith in each and every member of our Academic Team and I believe they will guide you towards enhancing your academic knowledge along with practicing your debating and negotiating skills through presenting the best environment for a spirit of diplomacy. Meanwhile, now that they can arrange physical challenges, coffee breaks and social events again, I believe our amazing and all-mighty Organization Team members are in a frenzy! They are working with great dedication to ensure that you leave TROYMUN 2026 with unforgettable memories and lots of new friends. Overall, we are all looking forward to meet you again!

On behalf of TROYMUN family and Parion Hotel, I would like to thank you for your time and consideration and once again, with great pleasure, welcome you to TROYMUN 2026. Do not forget to apply, to read your study guides, prepare some speeches and motions, and buckle your seatbelts for three days of fun, discussion, games and politics! In case of any questions, do not hesitate to contact us. We would be more than happy to help you. See you in November

Your Sincerely,

Baran Akarsu

Secretary-General of TroyMUN

II. Letter from Mentor Under-Secretary-General

I would like to start by thanking my teachers and the wonderful women who made the TROYMUN conferences possible for years Ms. Çağlayan Nazlıca and Ms. Arzu Kotan Deveci. I'm so thankful to be a part of this family and, even though once a year, work towards a shared goal.

I would also like to thank our Secretary-General Baran Akarsu for his efforts towards this conference. And my Under-Secretary-General Alperen Belek for his diligent work in preparation for his committees.

Dear delegates, I sincerely hope you will enjoy tackling current problems of cyber-crime this November. Remember to suit up and have fun. In a world filled with uncertainty I wish for a smooth sailing conference for everyone.

Yours truly,

Nur Elif Battal

Mentor Under-Secretary-General responsible for United Nations Office on Drugs and Crime

III. Letter from Under-Secretary-General

Esteemed Delegates,

First of all, I would like to welcome all of you to the ninth annual session of TroyMUN'26!

I am Alperen Belek and I will be serving as your Under-Secretary-General for this year's conference on the UNODC committee. I would also like to thank my supportive Mentor USG Nur Elif for guiding me and helping me whenever I needed it.

This year, UNODC welcomes you as a specialized committee with high energy and an unceasing pace. So get ready, because with this comprehensive study guide you'll be preparing for what might be the most exciting and impressive committee at the conference.

This year's agenda focuses on "Combating the Rise of Cyber-enabled Transnational Organized Crime and Darknet Marketplaces". As digital technologies continue to transform the way criminal networks operate, strengthening international cooperation and developing effective responses to these emerging threats is becoming increasingly important. As Chairboard, we look forward to seeing your passion, dedication, and energy throughout the committee. Also, enjoy every moment and make this experience one to remember

Lastly I would like to thank Ms. Çağlayan Nazlıca and Ms. Arzu Kotan Deveci for their years of efforts to make TroyMUN conferences a reality for all. And I also would like to thank my Secretary-General Baran Akarsu for supporting us until now.

With all my best,

Alperen Belek

Under-Secretary-General responsible for United Nations Office on Drugs and Crime

IV. Introduction to the Committee: United Nations Office on Drugs and Crime

Established in 1997, UNODC works to make the world safer from drugs, crime, terrorism and corruption. Guided by its mandate and the underpinning conventions on international drug control, transnational organized crime, corruption and cybercrime, UNODC works with Member States to promote justice and the rule of law and make communities safer and more resilient.



Through its network of field offices and headquarters in Vienna, the Office provides normative and technical support along with reliable data and analysis to inform policymaking and programmatic responses. UNODC's mandate areas encompass preventing and countering transnational organized crime, corruption and terrorism, addressing the world drug problem, and enhancing and strengthening criminal justice systems.

Serving as guardian of international conventions and Secretariat of global UN policy bodies on drugs, crime and corruption, UNODC ensures normative support for multilateral policymaking. UNODC research provides high-quality, essential evidence to inform decision-making and operational responses to multifaceted challenges in the fields of drugs and crime. Achieving and safeguarding peace, health, security and justice for all in a world of intertwined threats requires coordinated responses and shared responsibility. UNODC

facilitates and promotes networks of cooperation across borders to shape a safer, more just and prosperous world for both present and future generations. [1]

V. Introduction to the Agenda Item : Combating the Rise of Cyber-Enabled Transnational Organised Crime and Darknet Marketplaces

A. Overview of the Agenda

Transnational organized crime enabled by cyber capabilities has emerged as a growing concern for international security and law enforcement. The development of information and communication technologies has enabled organized criminal groups to communicate, coordinate activities and reach victims across national borders. Digital technology has expanded the geographical scope of crimes that were previously constrained by borders, offering new opportunities for criminal networks to operate transnationally. [2]

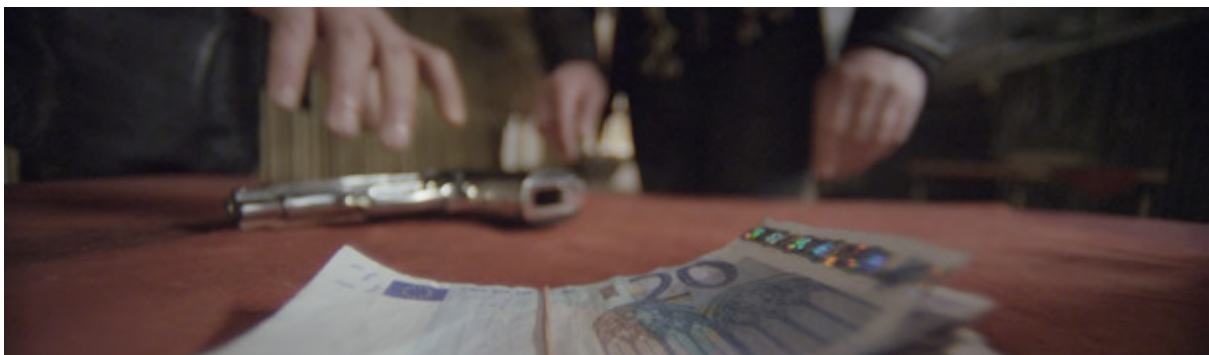
The Internet is also increasingly used to facilitate various forms of organized crime, such as fraud, trafficking, money laundering and illicit trade in goods and services. Darknet markets are one part of this larger picture. They are online venues for the purchase and sale of illegal goods and services, complicating law-enforcement investigations. UNODC notes that cyber organized crime may occur on the visible web and on the Deep Web including darknet sites. [3]

The transnational nature of these crimes poses significant challenges for national authorities, as perpetrators, victims, digital infrastructure and financial transactions may be in different countries. Therefore, in order to combat cyber-enabled organized crime, there is a need for international cooperation, effective legal structures, information sharing and coordinated responses from the criminal justice system. Thus, the UNODC's work on cyber organized crime not only aims at understanding how criminal groups use technology but also seeks to strengthen international efforts to prevent and counter these emerging forms of crime. [4]

B. Historical Background of the Agenda Item

1. The Evolution of Organized Crime

Organized crime has changed a lot due to globalization, technology and changing markets. Traditionally associated with relatively structured criminal groups, it has increasingly evolved into more flexible and networked forms, able to operate across national borders. UNODC states that transnational organized crime is a dynamic phenomenon, adapting to markets and creating new forms of criminal activity. [2]



The transnational nature of organized criminal activity prompted States to enhance cooperation through the **United Nations Convention against Transnational Organized Crime (UNTOC)**, adopted in 2000 and entered into force in 2003. UNTOC does not give a fixed definition of “organized crime”. Rather, it defines an organized criminal group as a structured group of three or more persons, that exists for a period of time and whose members act together with a view to committing serious crimes for financial or other material benefit. [5]

As criminal networks adapt to technological and global developments the line between traditional organized crime and newer forms of digitally facilitated crime has become more and more significant. This evolution provides the historical background for understanding the increasing incorporation of digital technologies in the activities of the organized criminal groups. [6]

2. The Rise of Cybercrime

The rapid growth of the Internet and information and communication technologies (ICTs) changed the nature and scale of criminal activity. Unlike many traditional crimes, cybercrime allows offenders to communicate with victims and other criminals across countries with greater speed and less effort, as it can cross physical and geographical boundaries. This also allowed organized criminal groups to use digital technologies to increase the scale of existing criminal activities and develop new forms of organization. [7]



Cyber-dependent crimes are distinguished from cyber-enabled crimes by UNODC. Cyber-dependent crimes can only be committed using computers, computer networks or other ICT systems, while **cyber-enabled** crimes are traditional crimes that are **enhanced** in scale or reach through the use of digital technologies. The distinction is of particular relevance to this agenda given the increasing use by organized criminal groups of ICTs to facilitate activities such as fraud, illicit trade and other transnational crimes. [8]

Criminal groups adapted to the digital environment and the internet have become a tool for organizing criminal activities, rather than just a tool to commit individual offenses. UNODC also observes that cyberspace may enable criminal groups to create temporary or more permanent networks, communicate with each other and access new online criminal markets. This evolution led to the rise of cyber-enabled transnational organized crime, which is the main subject of this agenda item. [9]

3. The Emergence of Darknet Marketplaces

The rise of the darknet was another stage in the evolution of cyber-enabled organized crime. Darknet sites are part of the Deep Web, and are designed to provide more anonymity than normal websites. Criminal actors have used this environment to communicate, organize activities and facilitate illicit trade across national borders. Cyber organized crime, UNODC reports, can occur on visible web and Deep Web sites including darknet sites. [3]

The rise of darknet marketplaces was particularly significant because of the development of cryptocurrencies and anonymity-enhancing technologies. One of the first, and largest, examples was Silk Road, launched in 2011, which showed how these technologies could be combined to support illicit online markets. The number of active darknet markets has grown from one in 2011 to 118 in 2019, according to UNODC, although individual markets are often short-lived and can disappear following law enforcement operations, hacks or voluntary closure. [10]

Darknet marketplaces have since evolved from single websites to broader criminal ecosystems. They can help the trading of illicit goods and services and allow criminal actors to communicate, build relationships and operate across borders. This has turned darknet marketplaces into a major part of today's cyber-enabled transnational organized crime and created new challenges for international law enforcement and criminal justice cooperation. [11]

4. International Response

The transnational character of organized crime supported by cyber technologies has become a reason to pay attention to international cooperation. There is a useful convention in this respect, namely the **United Nations Convention against Transnational Organized Crime (UNTOC)** that was adopted in 2000 and came into force in 2003. However, fast development of cybercrime required something more specific to be done. [1]

In December 2024, the United Nations General Assembly passed the United Nations Convention against Cybercrime, which was the first-ever global treaty on cybercrime. The main goal of the United Nations Convention against Cybercrime is to increase international cooperation in this field, as well as the exchange of electronic evidence and collaboration between law enforcement agencies. The work on implementing the treaty is done by UNODC. [12]

C. Sustainable Development Goals (UN SDG's)

Adopted by UN Member States in September 2015, the 2030 Agenda for Sustainable Development outlines 17 Sustainable Development Goals (SDGs).



Which aim at promoting sustainable development in economic, social and environmental aspects. These goals acknowledge the interconnectedness of peace, development, human rights, equality, and the rule of law. UNODC is instrumental in helping Member States deal

with drugs, crime, corruption, and terrorism, reinforcing justice and rule of law, and developing resilient societies. This organization's efforts have a particular connection with SDG 16, although other mandates and operations of the organization contribute towards the rest of the 2030 Agenda Goals. [13]

1. Goal 16 : Peace, Justice and Strong Institutions



Goal 16 is about promoting peaceful and inclusive societies, providing access to justice for all, and building effective, accountable, and inclusive institutions at all levels. People everywhere should live free from fear and all forms of violence, feeling safe as they go about their lives—regardless of their ethnicity, faith, or sexual orientation. [14]

This has a lot of relevance for the work that the UNODC does because organized crime, corruption and poor rule-of-law regimes are some of the things that can compromise the attainment of peace, justice and institutions. UNODC has made a direct contribution to SDG 16 in that it has helped Member States enhance their criminal justice systems, strengthen rule of law and deal with organized crime. Target 16.4 is very relevant for this item in particular because it calls upon states to “combat all forms of organized crime” and decrease illicit financial and arms flows. [15]

For this agenda item, SDG 16 offers a direct link between cyber-enabled transnational organized crime and the overall mission of the United Nations to strengthen justice and institutions. [16]

2. Goal 17 : Partnerships for the Goals



Goal 17 is about revitalizing the global partnership for sustainable development. The Sustainable Development Goals (SDGs) are a universal blueprint and a call to action for all countries—both developed and developing—to ensure no one is left behind. Achieving them requires active partnerships between governments, the private sector, and civil society. [17]

It is directly linked to the UNODC in that the fight against transnational organised crime involves cooperation between governments, international institutions, civil society, academia, and the private sector. The UNODC promotes such an effort through creating multi-stakeholder partnerships and assisting Member States in increasing their cooperation and coherence in fighting organized crime and related criminality. [18]

In relation to the current agenda item, SDG 17 becomes highly relevant since cyber-enabled transnational organised crime involves the crossing of national and jurisdictional borders. Therefore, international cooperation, capacity development, knowledge exchange, and partnership become necessary to enhance countries' capacities to prevent and investigate these crimes. The UNODC's efforts under Target 17.9, 17.16 and 17.17 are relevant in this regard. [18]

3. Goal 8 : Decent Work and Economic Growth



Goal 8 of Sustainable Development Goals (SDGs 8) seeks to foster inclusive and sustainable economic growth, full and productive employment, and decent work for all. The relationship between this goal and UNODC is less direct than that between SDG 16 and UNODC because the main mandate of UNODC centers on drugs, crime, corruption, terrorism, and criminal justice. Nevertheless, organized crime can threaten the economic activities of legitimate businesses and take advantage of vulnerable employees, hence the relevance of anti-trafficking efforts to SDG 8. [2]

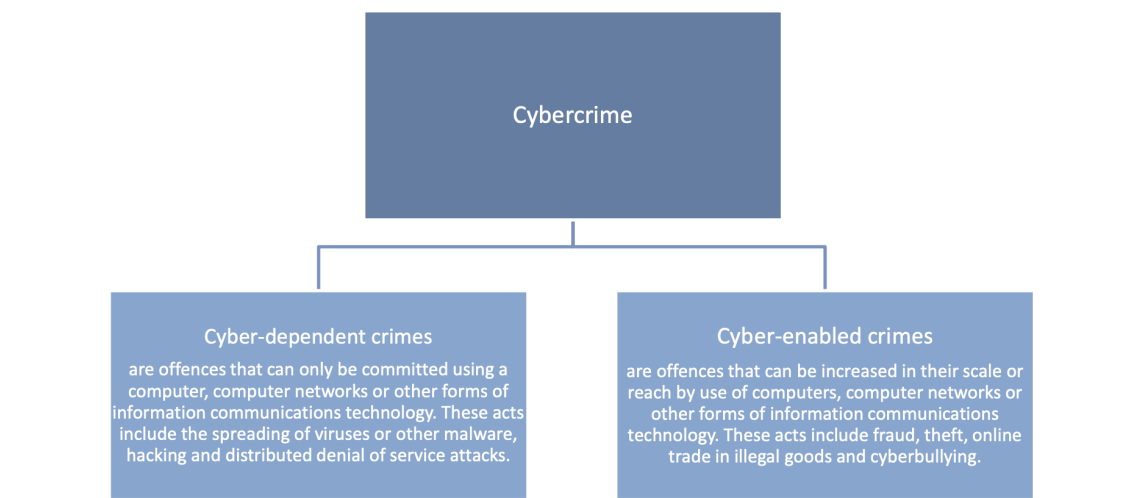
Specifically, Target 8.7 covers forced labor, modern slavery and human trafficking, all issues where the UNODC assists the Member States. Consequently, although SDG 8 is not the primary SDG relevant to this issue area, it is supportive in its coverage of certain economic and social factors that relate to organized crime. [19]

In general, SDG 8 has an indirect but pertinent link to the work of UNODC. The fight against organized crime, human trafficking and exploitation is not the main SDG for this agenda item, but it can contribute to better security of economic environments and decent working conditions. SDG 8 can thus be considered a supporting SDG together with the more directly relevant SDG 16 and SDG 17.

D. Understanding Cyber-Enabled Organized Crime and Darknet Marketplaces

1. Cyber-Enabled vs Cyber-Dependent Crime

Generally, cybercrime can be classified as cyber-dependent and cyber-enabled crime based on the role of information and communication technologies (ICTs). Cyber-dependent crimes are crimes which can only be committed through the use of computers, computer networks or other digital technologies. They directly target computer systems and data and their confidentiality, integrity or availability, namely hacking, malware attacks and Distributed Denial-of-Service (DDoS) attacks. [20]



Cyber-enabled crime, in contrast, refers to traditional crime that is enhanced by the use of ICTs in terms of its scale or reach. Examples are online fraud, illegal online trade and money laundering. The main difference is therefore whether technology is part of the crime itself or whether it is used to facilitate or extend an existing form of crime. [21]

This distinction is of particular importance for this agenda item, as organized criminal groups increasingly use digital technologies to expand activities that previously happened offline. Understanding the difference helps individuals in government and law enforcement determine appropriate legal, investigative and international responses to different types of cybercrime. [9]

2. Characteristics of Cyber-Enabled Organized Crime

Cyber-enabled organized crime is the use of digital technologies to facilitate, expand and coordinate criminal activities across borders. When compared to cyber-dependent crimes, the underlying criminal activity may exist without technology, but ICTs enable organized criminal groups to operate on a much larger scale and reach victims, markets and partners in different countries. [9]

A major feature of cyber-enabled organized crime is its transnational nature. Criminal groups can communicate, coordinate their operations and carry out financial transactions across jurisdictions, while different stages of a criminal activity can happen in different countries. This creates major difficulties for law enforcement agencies, especially when investigating crimes involving multiple legal systems. [22]

Another trait of cyber-enabled organized crime is that it has a flexible and networked organizational structure. Through the use of digital technology, it is possible for the criminals to collaborate in the absence of being in the same country or having any traditional form of hierarchical organization. The criminals might also make use of cyberspace to coordinate and recruit. [23]

The other critical feature is the capacity for rapid adaptation to technological changes. Organized criminals can make use of emerging digital technology and techniques, thereby making their operations harder to track and investigate. For this reason, the fight against cyber-based organized crimes not only involves efficient law enforcement strategies but also requires international collaboration and constant adaptation of laws and investigative techniques. [24]

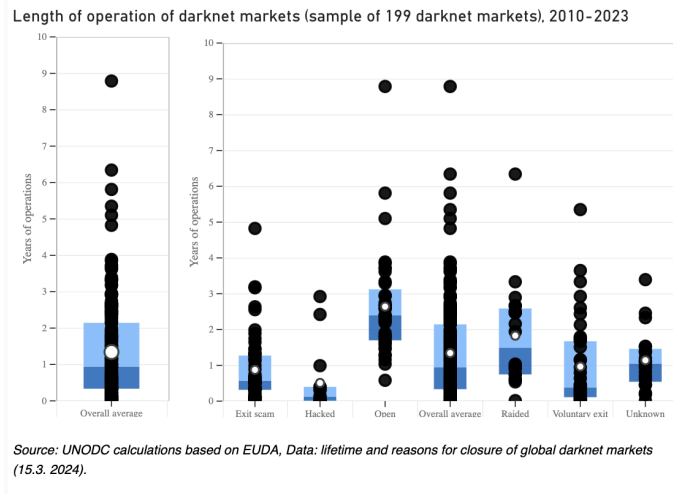
3. How Darknet Marketplaces Operate

Darknet marketplaces are websites operating in the darknet portion of the Internet, which offers increased anonymity compared to the surface web. Darknet marketplaces operate in much the same way as traditional e-commerce sites do, as far as their basic architecture is concerned, since vendors can market their products or services while buyers can connect to the vendors and perform their transactions on such websites. However, darknet marketplaces deal mostly in illicit products and services, which creates problems for the law enforcement agencies. [25]

Among the most significant characteristics of darknet marketplaces is the use of anonymity-assuring technology and cryptocurrencies. The report by the UNODC notes that marketplaces utilize technology that hides the identity or location of its users, and cryptocurrency acts as an instrument for payments. [26]

Escrow and reputation systems are also used on darknet marketplaces to enable transactions. In the escrow system, the payment is made to the website, and it is only released once the transaction is completed. On the other hand, the reputation system enables individuals to give ratings to the vendors using their previous transactions. This system ensures that there is some trust between anonymous parties. [25]

Another very significant aspect of the darknet is the impermanence and extreme flexibility of such marketplaces. Markets can be shut down due to interventions by law enforcement agencies or through technical attack or even due to their own closure or due to frauds committed. The recently conducted research by UNODC indicates that the darknet markets are extremely volatile and have relatively short life spans. [10]



This business model is very applicable to cyber-enabled transnational organized crime because it can link criminal elements from different nations together, allowing them to exchange illegal commodities or services and even

facilitating communication and networking. For this reason, any efforts aimed at disrupting these marketplaces will need international collaboration. [11]

4. Common Criminal Activities

Cyber-enabled organized crime is defined as a broad category of criminal activity where digital technologies are used to facilitate, extend or coordinate organized crime. Common activities include **online fraud, identity crimes, blackmail and extortion, intellectual property crime, money laundering and illicit trafficking**. [3]

When criminal groups attempt **online fraud and identity related crime** they may use digital technologies to access and misuse personal or financial information, posing significant financial and security risks to individuals, businesses and institutions. [23]



Another important criminal activity is **money laundering**. Digital technologies can help move criminal proceeds across jurisdictions and hide them. This complicates financial investigations and can reinforce the overall financial structure of

transnational criminal networks. [3]

Cyber-enabled technologies can also facilitate illicit trafficking and **criminal markets online**. UNODC identified activities including trafficking in persons, smuggling of migrants, wildlife trafficking and other illicit trade as forms of organized crime that can be facilitated through ICTs. [3]

Finally, **crime-as-a-service** allows criminal actors to access specialized tools, data or services from other criminals. This can increase the flexibility of cyber-enabled organized crime and enable different actors to contribute to different stages of criminal activity. [3]

5. Why Darknet Marketplaces are Difficult to Combat

Darknet marketplaces are difficult to combat simply because they often use technologies that make it more difficult to identify and monitor users, communications and online activities. Their content is also mostly unindexed so traditional search engines can not really find it. [42]

Another big problem is the transnationality of these markets. Criminal actors, digital infrastructure, financial transactions and victims may be located in different jurisdictions, so

that investigations depend on international cooperation and on timely access to information. National laws and investigative capacities may differ, further complicating these efforts. [27]

The use of cryptocurrencies and encrypted communications may also limit the ability of authorities to trace financial activity and establish links between criminal actors. Darknet markets are also quick to adapt to disruptions, with users and vendors moving to new platforms. [28]

Finally, law enforcement agencies may face limitations in technical expertise, digital-forensic capacity, resources and international information-sharing. Therefore, the fight against darknet marketplaces requires not only law enforcement operations but also enhanced international cooperation, specialized training, technological capacity and effective legal structures. [27]

E. Current Challenges

1. Ransomware

A ransomware is a type of malicious software that limits one's access to their information and asks for some kind of monetary reward in exchange for gaining such access back. Initially aimed at individuals, the use of ransomware has recently been expanding into corporate settings, public institutions and organizations responsible for providing essential services. [29]



A ransomware represents a serious problem to deal with in terms of fighting cybercrime due to its serious consequences that include not only damage to the IT system but also material losses. [30]

Its international dimension makes matters even more complicated for investigations. The criminal, the victim, the computer infrastructure used and the transactions may be based in different countries, thus necessitating cooperation between the various stakeholders. [30]

For UNODC and the member states, this means that responding to ransomware attacks would require better international cooperation, legal frameworks, investigation capabilities and cybersecurity measures. [30]



2. Cryptocurrency-based Money Laundering

Cryptocurrencies may be exploited for money laundering because such funds could be laundered by making transfers and conversion in digital finance channels. The international nature of cryptocurrencies, along with, at times, the anonymity of the users involved, may present further complications for law enforcement agencies investigating financial crimes. [31]

The above concern becomes even more pertinent with respect to the organised crime that has the cyber component since there are various ways of using cryptocurrencies in such

situations, which can allow for transferring of proceeds internationally and tying up financial activity with other crimes in cyberspace. [31]

One of the major issues is the fact that virtual assets operate in a **transnational and decentralized manner**. There might be different jurisdictions and various regulatory frameworks involved in investigation, as well as various problems with collecting the necessary financial or digital evidence. [32]

Therefore, fighting money laundering through cryptocurrencies calls for **greater cooperation among nations, regulating virtual asset service providers and intelligence sharing in finance**. UNODC highlights capacity-building and cooperation on matters such as conducting investigations that are blockchain-specific and tracking and recovering illegal virtual assets. [32]

3. AI-Assisted Cybercrime

The use of artificial intelligence is becoming more common among criminals in order to boost the efficacy of their cyber crimes. Artificial intelligence can be employed in performing activities such as committing **fraud, phishing, impersonation, and even creation of false information**. [33]



The other issue that has emerged is that of the **generative AI and deepfakes**. Criminal organizations have the potential to leverage generative AI to produce fake texts and images, which would result in more convincing impersonations and social engineering attempts.

It will be harder to identify such fraudulent communications in the future. [34]

Also, AI can be leveraged to automate and scale criminal activities. According to UNODC, AI-enabled tools allow automating some forms of cyber-enabled crime and thus help the criminal organizations target more victims at once. [33]

For UNODC and member states, the increasing adoption of artificial intelligence by cybercriminals brings about difficulties in terms of law enforcement and cyber investigations. The solution to the problems is to build robust investigative capabilities and information exchange, and adopt suitable legal instruments. [33]

4. Cross-Border Investigations

Cyber-enabled transnational organized crime is defined by the involvement of criminal actors, victims, digital infrastructure, and electronic evidence in different countries. This makes cross-border investigations essential, as national authorities may not have direct jurisdiction over all aspects of a case. [29]

The temporary nature of electronic evidence presents a major obstacle. Foreign service provider data may need to be preserved and acquired quickly, but differences in national laws and procedures can delay investigations. Mutual legal assistance and international cooperation mechanisms are therefore important for the purpose of collecting evidence in a lawful and efficient manner. [38]

Successful cross-border investigations also depend on cooperation between law enforcement agencies, prosecutors, judicial authorities and private tech companies. The UNODC highlights mechanisms like 24/7 networks, information-sharing and coordinated procedures for requesting electronic evidence across jurisdictions. [37]

For UNODC and Member States, enhancing cross-border investigations requires harmonized legal structures, specialized training, enhanced digital-forensic capacity and faster international cooperation. The United Nations Convention against Cybercrime also emphasizes the importance of international cooperation and exchange of electronic evidence in investigations. The United Nations Convention against Cybercrime further emphasizes international cooperation and the sharing of electronic evidence in investigations of serious crime. [37]

5. Data Sharing and Digital Evidence

Digital evidence is crucial for the investigation of cyber-enabled transnational organized crime, but it is often stored in multiple countries, devices and online services. Its effective use therefore depends on the timely preservation, collection and sharing of electronic evidence between relevant authorities. [29]

Law enforcement agencies, prosecutors, judicial authorities and service providers need to cooperate internationally to obtain evidence in a lawful and efficient manner. UNODC highlights information sharing, 24/7 cooperation networks and mutual legal assistance as important tools for cross-border investigations. [37]

In 2024, the United Nations Convention against Cybercrime further strengthened the international framework for cooperation and the sharing of electronic evidence in investigations of serious crimes. [38]

6. Public-Private Cooperation

Critical digital infrastructure, platforms and electronic data are often owned by private companies, so public-private cooperation is essential to combat cyber-enabled organized crime. Governments, law enforcement agencies and technology companies can therefore work together to better detect, investigate and prevent cybercrime. [39]



Private-sector organizations can bring specialist expertise and relevant data and digital-forensic capabilities that are not always available to public authorities. As UNODC notes, effective cybercrime investigations and information sharing are importantly strengthened by partnerships with internet and technology

companies. [40]

But privacy requirements, different legal structures, and difficulties requesting electronic evidence across borders can make cooperation difficult. The UNODC highlighted the need for streamlining data requests and establishing confidence and common procedures between public and private actors as key areas for improvement. [41]

It is for this reason that Member States should ensure the development of sound legal frameworks, robust information exchange processes, and sound public-private partnership structures. Cooperation will assist authorities in dealing with new cybersecurity challenges while ensuring that information exchange and its usage comply with the existing laws. [38]

F. Existing International Frameworks

Existing international legal frameworks are necessary for dealing with the problems of cyber-enabled transnational organized crime since the nature of criminal activities, as well as digital evidence, usually involves crossing the borders of different countries. It ensures the necessary legal instruments for cooperation, sharing of information, investigations and prosecutions among States. UNODC stresses that **proper international cooperation** requires corresponding legal and cooperation frameworks. [26]

1. United Nations Convention against Transnational Organized Crime (Palermo Convention)

The United Nations Convention against Transnational Organized Crime (UNTOC), also known as the Palermo Convention, was adopted by the UN General Assembly on 15 November 2000, and entered into force on 29 September 2003. It is the main



international legal instrument to fight transnational organized crime and it provides a framework for international cooperation between States. [43]

The Convention urges States Parties to strengthen measures to combat organized crime, including through the criminalization of participation **in organized criminal groups and of money laundering and corruption**, and the establishment of mechanisms for extradition, mutual legal assistance and law-enforcement cooperation. It is supplemented by three Protocols on trafficking in persons, smuggling of migrants and trafficking in illicit firearms. [18]

In relation to this agenda, the Palermo Convention is highly pertinent due to the fact that cyber-enabled organized crime often functions on a transboundary level. Despite the fact that this convention was formulated prior to cybercrime, it does serve as an important basis in dealing with transnational criminal organizations using cyber technology. [18]

2. Budapest Convention on Cybercrime



The Budapest Convention on Cybercrime, (officially the Council of Europe Convention on Cybercrime) was adopted in **2001** and entered into force in **2004**. It was the first international treaty specifically dealing with cybercrime and

electronic evidence and provides a framework for harmonizing national legislation and strengthening international cooperation. [44]

The Convention has articles relating to **the criminalization of cybercrime, investigation of cyber crime and collection of electronic evidence**. Furthermore, it provides for cooperation between countries, which is very crucial for cross border crimes. [45]

The Convention is especially pertinent to this agenda as cyber-enabled organized crime often involves electronic evidence in different jurisdictions. Its Second Additional Protocol, adopted to strengthen cooperation and the exchange of electronic evidence, addresses additional challenges including cross-border access to data and cooperation with service providers. [46]

3. INTERPOL & Europol Operations



INTERPOL and Europol have key roles to play in coordinating international responses to cyber-enabled organized crime. INTERPOL facilitates the cooperation of law enforcement agencies worldwide by sharing threat intelligence, providing technical assistance

and coordinating cross-border operations. Its cybercrime activity is concentrated on threats like ransomware, online fraud and malware. [47]

In the EU, Europol's **European Cybercrime Center (EC3)** offers operational, analytical and digital-forensic support to the Member States. Its **Joint Cybercrime Action Taskforce (J-CAT)** brings together investigators from various jurisdictions and enables coordinated cross-border investigations into major cybercrime threats. [48]

These operations demonstrate the value of sharing **real-time intelligence, joint investigations and cooperation in international law enforcement**. Cyber-enabled organized crime is becoming more cross-jurisdictional with organizations such as INTERPOL and Europol helping national authorities to pool resources and respond more effectively to transnational threats. [48]

4. UNODC Global Programme on Cybercrime



The UNODC Global Program on Cybercrime, supports Member States to prevent and combat cybercrime through enhancing their criminal justice and law enforcement capacities. The Program offers **technical assistance, capacity-building, legal support, international cooperation and research** to assist countries in addressing cyber-dependent and cyber-enabled crime. [49]

The Program is a major emphasis of developing the skills and resources needed for **cybercrime investigations and digital evidence** for national authorities. It also further

encourages prevention and awareness-raising, cooperation between relevant institutions and the development of sound legal and policy frameworks. [49]

The Program is of particular relevance to this agenda, as it supports Member States in strengthening their capacity to respond to **transnational cybercrime and organized criminal networks working through digital technologies**. Its capacity-building and international cooperation activities support the larger international framework presented in this section. [49]

5. FATF Standards on Virtual Assets



The Financial Action Task Force (FATF) has developed international standards to reduce the risks of money laundering and the financing of terrorism associated with digital assets. **Recommendation 15** calls on countries to regulate **Virtual Asset Service Providers (VASPs)** and establish sufficient anti-money laundering and counter-terrorist financing measures.[50]

These standards require that VASPs be **licensed or registered, supervised and subject to risk-based controls**. They also support customer identification, record-keeping and sharing of relevant information on virtual-asset transfers. [50]

The FATF standards are especially relevant to this agenda because cryptocurrencies can be used to transfer and hide the proceeds of cyber-enabled crime across borders. Therefore, effective implementation contributes to strengthening financial monitoring, international cooperation and the ability of authorities to identify and disrupt illicit financial flows. [51]

6. Regional Cooperation Mechanisms

Mechanisms for regional cooperation are important to address cyber-enabled transnational organized crime because criminal networks and digital evidence often cross national borders. Regional frameworks can enable **information sharing, joint investigations, mutual legal assistance and cooperation between law-enforcement authorities**. [29]

Organizations and regional frameworks such as the **European Union, ASEAN, African Union and Organization of American States** have developed mechanisms to enhance cooperation against cybercrime and other forms of transnational crime. These mechanisms can also help in capacity building and in sharing of technical expertise among Member States. [52]

In this regard, improved regional cooperation will allow states to react faster to transnational crimes and facilitate better access to digital evidence. Cooperation at regional and international levels is critical to tackling cybercrime due to its transnational character, which requires proper legal framework and information sharing networks. [29]

G. Emerging Trends

Cyber-enabled organized crime is undergoing rapid changes due to adoption of newer techniques by the criminal groups. Some emerging trends include **artificial intelligence, automation, deepfake and virtual assets**, which make it necessary for the law enforcement agencies and policymakers to constantly update themselves on how to handle such issues. [33]

1. AI-powered Criminal Activities

Criminal networks increasingly automate and scale existing forms of cyber-enabled crime with artificial intelligence. That means more convincing fraud and impersonation, automated phishing, deepfake-powered scams and other social engineering attacks, leading to faster and more adaptable criminal operations. [33]

The concern isn't about the creation of new types of crime but rather about AI's ability to scale up, streamline and improve on existing criminal activity. This makes AI an important emerging challenge for law enforcement agencies and policy makers. [33]

2. Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) is a cybercrime business model where specialized criminal actors develop and offer ransomware to affiliates who carry out attacks. This division of labor allows those with limited technical skills to participate in ransomware activities and improves the scalability and organization of cybercrime. [33]

RaaS is an example of cybercrime being organized into specialized networks with different actors responsible for developing tools, conducting attacks and managing financial activities. This model could make ransomware groups more adaptable and more difficult for law enforcement to disrupt. [33]

3. Decentralized Darknet Marketplaces

Darknet marketplaces are becoming increasingly decentralized and fragmented and criminal activity is becoming less reliant on a few large platforms. The darknet market scene has

become more fragmented, with smaller, shorter-lived markets popping up in the wake of disruptions to major platforms, UNODC states. [10]

This trend can hinder law enforcement because if one marketplace is disrupted, the wider criminal network may still be running. Instead, criminal actors can switch between platforms and stay connected through decentralized networks, making attribution and coordinated investigations harder. [26]

Therefore, it is becoming increasingly important to fight decentralized darknet markets through international intelligence sharing, coordinated investigations and flexible law-enforcement strategies rather than by targeting individual platforms. [10]

4. Privacy Coins and Cryptocurrency Mixers



Privacy coins and crypto mixers could further complicate matters for authorities investigating illicit financial activity. Cryptocurrencies that focus on privacy can provide better transaction privacy, and mixers can make it harder to link the source of funds to their destination. [25]

These technologies can be used to cover up proceeds of cybercrime and other forms of organized crime and to hinder financial investigations and the tracing of illicit assets across jurisdictions. However, their usage represents only a small percentage of the overall legitimate virtual-asset ecosystem. [31]

To address these risks, Member States need to enhance financial intelligence, international cooperation and appropriate regulation of virtual-asset services, while preserving the legitimate use of digital financial technologies. [31]

5. Future Challenges for International Law Enforcement

With each passing day, international law enforcement will face the challenge of cybercriminal networks that are increasingly sophisticated, decentralized and transnational. The growing deployment of AI, ransomware, anonymity-enhancing technologies and rapidly changing digital tool landscape can add complexity to investigations and impose new demands on specialized expertise. [53]

Another major challenge is keeping legal and investigative frameworks up to date with technological developments. Differences in national laws, difficulties in obtaining cross-border electronic evidence and the speed at which digital data can vanish may impede investigations and prosecutions. [37]



Future responses will thus need more international information-sharing, swifter cooperation, advanced digital-forensic capabilities, and closer public-private partnerships.

Law enforcement agencies will also need to continually adapt their methods and develop new technological capabilities to keep pace with evolving criminal threats. [54]

VI. Case Studies

Some of the news, events, and documents in this section provide you with information about the agenda item.

1-) Qakbot International Operation (2023) - Cross-border investigation -

<https://www.europol.europa.eu/media-press/newsroom/news/qakbot-botnet-infrastructure-shattered-after-international-operation>

2-) Operation Bayonet – AlphaBay & Hansa (2017) - Darknet -

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-13/key-issues/preventing-and-countering-cyber-organized-crime.html>

3-) AudiA6 Cryptocurrency-Laundering Operation (2026) - Cryptocurrency Laundering -

<https://www.europol.europa.eu/media-press/newsroom/news/ransomware-gangs-cut-euro-336-million-audi-a6-crypto-laundering-pipeline>

4-) Operation Cronos – LockBit (2024) - Ransomware (RaaS) -

<https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>

5-) Global Action against Online Fraudsters in the Airline Sector (2014) - Public-Private Cooperation -

<https://sherloc.unodc.org/cld/ar/education/tertiary/organized-crime/module-8/exercises/case-studies.html>

6-) Operation LadyBird – Emotet (2021) - Cybercrime-as-a-Service -

<https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>

VII. Questions to Ponder

1. What measures can be taken to disrupt the financial networks supporting cyber-enabled organized crime?
2. How can governments combat ransomware and Ransomware-as-a-Service without disrupting legitimate digital services?
3. What role should technology companies and other private-sector actors play in combating cybercrime?
4. How can UNODC and other international organizations support countries with limited technical and investigative capacities in combating cybercrime?
5. How can international legal frameworks keep pace with rapidly evolving technologies used by criminal networks?
6. How can law-enforcement agencies disrupt darknet marketplaces while respecting privacy and legitimate uses of anonymity technologies?
7. How can cryptocurrencies and virtual assets be prevented from facilitating money laundering and illicit financial flows?
8. How can States prevent artificial intelligence from increasing the scale and sophistication of cyber-enabled organized crime?
9. How can international investigations overcome jurisdictional barriers when criminals, victims and digital evidence are located in different countries?
10. What mechanisms are needed to ensure the rapid preservation and lawful sharing of electronic evidence between States?

VIII. Further Reading

This section contains resources that can assist you during the committee sessions.

1. Darknet Cybercrime Threats to Southeast Asia

https://www.unodc.org/roseap/uploads/archive/documents/Publications/2021/Darknet_Cyber_crime_Threats_to_Southeast_Asia_report.pdf

2. The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean

https://www.unodc.org/res/opioid-crisis/index_html/08_OnlineTrafficking_Report_Revised.pdf

3. What's the Difference between Europol and Interpol

<https://www.europol.europa.eu/faq/europol%E2%80%A6interpol%E2%80%A6what%E2%80%99s-difference>

4. The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia

https://www.unodc.org/documents/Reports/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf

5. AI is Turbocharging Organized Crime, EU Police Agency Warns

<https://apnews.com/article/europe-crime-europol-ai-security-cyber-attack-846847536f6feb2bb423943fd96e1f1>

6. Japan's Asahi hack that halted beer production claimed by Qilin ransomware group

<https://www.reuters.com/world/asia-pacific/cybercriminals-claim-hack-japans-asahi-group-2025-10-07/>

7. Party's over for crypto scammers who went on a spending after a \$240 million bitcoin theft

<https://apnews.com/article/cryptocurrency-scam-malone-lam-guilty-3d40f81fd3ba0b5e28d6b962ca6b343d>

IX. Bibliography

[1] United Nations Office on Drugs and Crime (UNODC). *UNODC Annual Report 2024*.

https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf

[2] United Nations Office on Drugs and Crime (UNODC). *Organized Crime*.

Kevin.Town. (n.d.). *Transnational organized crime: the globalized illegal economy*.

<https://www.unodc.org/toc/en/crimes/organized-crime.html>

[3] UNODC SHERLOC. *Introduction to Cybercrime*.

Organized Crime / Cybercrime Module 13 Key issues. (n.d.).

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-13/key-issues/intro.html>

[4] UNODC SHERLOC. *Cybercrime: Introduction and Learning Outcomes*.

Organized Crime / Cybercrime Module 13 Introduction and learning Outcomes. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-13/introduction-and-learning-outcomes.html>

[5] UNODC. *United Nations Convention against Transnational Organized Crime (UNTOC)*.

United Nations Convention against Transnational Organized Crime. (n.d.)

<https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>

[6] UNODC SHERLOC. *Conceptualizing Organized Crime and Defining the Actors Involved*.

Organized Crime / Cybercrime Module 13 Key issues: Conceptualizing organized crime and defining the actors involved. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-13/key-issues/conceptualizing-organized-crime-and-defining-the-actors-involved.html>

[7] UNODC SHERLOC. *Cybercrime in Brief.*

Cybercrime Module 1 Key issues: Cybercrime in brief. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-1/key-issues/cybercrime-in-brief.html>

[8] UNODC. *Organized Crime Lesson Handout: Cybercrime.*

https://www.unodc.org/documents/e4j/Secondary/Organized_Crime_Lesson_handout_cybercrime.pdf

[9] UNODC SHERLOC. *Cyber-Organized Crime: What Is It?*

Organized Crime / Cybercrime Module 13 Key Issues: Cyber Organized Crime: What is it? (n.d.)

https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

[10] UNODC. *World Drug Report 2026.*

WDR 2026 | Data Portal UNODC. (n.d.)

<https://data.unodc.org/wdr2026?page=6>

[11]. UNODC SHERLOC — Conclusion: Cybercrime and Organized Crime

Organized Crime / Cybercrime Module 13 Key issues: Conclusion. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-13/key-issues/conclusion.html>

[12]. UNODC — FAQ on the United Nations Convention against Cybercrime

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/FAQ_on_AH_C_December_2024.pdf

[13]. International Maritime Organization (IMO) — Sustainable Development Goals

IMO and the Sustainable Development Goals. (n.d.)

<https://www.imo.org/en/mediacentre/hottopics/pages/sustainabledevelopmentgoals.aspx>

[14]. United Nations — Goal 16: Peace, Justice and Strong Institutions

Stockton, M. (2026, September 14). *Goal 16: Peace, justice and strong institutions - United Nations Sustainable Development.*

<https://www.un.org/sustainabledevelopment/peace-justice/>

[15]. UNODC — Tools and Publications Relevant to the Sustainable Development Goals

https://www.unodc.org/documents/SDGs/UNODC_Tools_and_Publications_Relevant_to_SDGs_03-04-2020.pdf

[16]. UNODC — New York Newsletter, Q2 2024

https://www.unodc.org/documents/newyork/Newsletter/2024_Q2_Newsletter_.pdf

[17]. United Nations — Goal 17: Global Partnerships

Stockton, M. (2026b, September 14). *Goal 17: Partnerships for the Goals - United Nations Sustainable Development.*

<https://www.un.org/sustainabledevelopment/globalpartnerships/>

[18]. UNODC — Civil Society Guide / Interactive Resource

<https://www.unodc.org/documents/NGO/SE4U/UNODC-CSG-Interactive.pdf>

[19]. UNODC SHERLOC — Macro Perspective in Addressing the Smuggling of Migrants

Trafficking in Persons & Smuggling of Migrants Module 4 Key Issues: Macro-perspective in addressing smuggling of migrants. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/tip-and-som/module-4/key-issues/macro-perspective-in-addressing-smuggling-of-migrants.html>

[20]. UNODC SHERLOC — Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems

Cybercrime Module 2 Key Issues: Offences against the confidentiality, integrity and availability of computer data and systems. (n.d.)

<https://sherloc.unodc.org/cld/fr/education/tertiary/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html>

[21]. UNODC — Organized Crime Lesson Handout: Cybercrime

https://www.unodc.org/documents/e4j/Secondary/Organized_Crime_Lesson_handout_cybercrime.pdf

[22]. UNODC — Strategic Planning and Organized Crime: 2025 Report

https://www.unodc.org/documents/data-and-analysis/tocta/Brief_2025/SPOI_Organized_Crime_2025.pdf

[23]. UNODC SHERLOC — Criminal Groups Engaging in Cyber-Organized Crime

Organized Crime / CyBercrime Module 13 Key issues: Criminal groups engaging in Cyber

Organized crime. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html>

[24]. UNODC SHERLOC — Organized Crime Approaches

Organized Crime Module 12 Key issues: Organized Crime Approaches. (n.d.)

<https://sherloc.unodc.org/cld/es/education/tertiary/organized-crime/module-12/key-issues/organized-crime-approaches.html>

[25]. UNODC — Darknet Cybercrime: Threats to Southeast Asia

https://www.unodc.org/roseap/uploads/archive/documents/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf

[26]. UNODC — Cybercrime and Organized Crime: Expert Group Report

https://www.unodc.org/documents/Cybercrime/IEG_Cyber_website/A_CONF.234_11_E.pdf

[27]. UNODC — Commission on Narcotic Drugs, 67th Session: Document

ECN.7/2024/CRP.1

https://www.unodc.org/documents/commissions/CND/CND_Sessions/CND_67/Documents/ECN72024_CRP1.pdf

[28]. UNODC — Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean

https://syntheticdrugs.unodc.org/uploads/syntheticdrugs/res/library/cybercrime_html/Online_Trafficking_of_Synthetic_Drugs_and_Synthetic_Opioids_in_Latin_America_and_the_Caribbean.pdf

[29]. UNODC SHERLOC — Cybercrime Trends

Cybercrime Module 1 Key issues: Cybercrime Trends. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-1/key-issues/cybercrime-trends.html>

[30]. UNODC — Ransomware: Ad Hoc Committee Document

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/0902-Ransomware-Agenda0826.pdf

[31]. UNODC — International Cooperation, 2025: CTOC/COP Working Group Document

https://www.unodc.org/documents/treaties/International_Cooperation_2025/4/CTOC_COP_WG.3_2025_4_E.pdf

[32]. UNODC — International Cooperation, 2025: CTOC/COP Working Group Document

https://www.unodc.org/documents/treaties/International_Cooperation_2025/5/CTOC_COP_WG.3_2025_5_E.pdf

[33]. UNODC — The Intersection of Criminal and Technological Innovation in the Use of Automation and AI

[https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats - The intersection of criminal and technological innovation in the use of automation and AI.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf)

[34]. UNODC — Transnational Organized Crime and the Convergence of Cybercrime and Other Criminal Activities

https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

[35]. UNODC — Cybercrime: Module 7 Introduction

Cybercrime Module 7 Key issues. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-7/key-issues/intro.html>

[36]. UNODC — Cybercrime: Expert Group Report, 2019

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_E.pdf

[37]. UNODC — Cybercrime Expert Group Document, 2021

<https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101012.pdf>

[38]. United Nations Treaty Collection — Treaty Events

UNTC. (n.d.)

https://treaties.un.org/Pages/TreatyEvents.aspx?path=Treaty/PastTreaty/Page1_en.html

[39]. UNODC SHERLOC — Who Conducts Cybercrime Investigations?

Cybercrime Module 5 Key issues: Who conducts cybercrime investigations? (n.d.)

<https://sherloc.unodc.org/cld/es/education/tertiary/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html>

[40]. UNODC SHERLOC — Informal International Cooperation Mechanisms

Cybercrime Module 7 Key issues: Informal international cooperation Mechanisms. (n.d.)

<https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-7/key-issues/informal-international-cooperation-mechanisms.html>

[41]. UNODC — Cybercrime: Civil Society and Private Sector Resource

<https://www.unodc.org/documents/NGO/CSU-CyberCrime-240731-WEB.pdf>

[42]. UNODC SHERLOC — Formal International Cooperation Mechanisms

Cybercrime Module 7 Key issues: Formal international cooperation Mechanisms. (n.d.)

<https://sherloc.unodc.org/cld/fr/education/tertiary/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html>

[43]. UNODC — UNTOC at 20

https://www.unodc.org/documents/treaties/UNTOC/COP/SESSION_10/Website/Practical_info/UNTOC_at_20.pdf

[44]. Council of Europe — Budapest Convention on Cybercrime

<https://www.coe.int/en/web/cybercrime/the-budapest-convention>

[45]. Council of Europe — Convention on Cybercrime

<https://www.coe.int/en/web/cybercrime/convention-on-cybercrime>

[46]. Council of Europe — Second Additional Protocol to the Budapest Convention

<https://www.coe.int/en/web/cybercrime/second-additional-protocol>

[47]. INTERPOL — Cybercrime: Our Response

Cybercrime – our response. (n.d.)

<https://www.interpol.int/Crimes/Cybercrime/Cybercrime-our-response>

[48]. Europol — European Cybercrime Centre (EC3): Structure and Collaboration

Europol. (2026, July 8). *European Cybercrime Centre: Structure and collaboration.*

<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/european-cybercrime-centre-structure-and-collaboration>

[49]. UNODC — Global Programme on Cybercrime Training Catalogue

https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf

[50]. FATF — 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs

<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf>

[51]. FATF — FATF Recommendations

<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>

[52]. UNODC — Comprehensive Study on Cybercrime

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/Cybercrime_report_2017/Report_Cyber_E.pdf

[53]. INTERPOL — New Cyberthreat Assessment for Asia and the South Pacific, 2026

New INTERPOL report highlights escalating cyber threats across Asia and South Pacific.

(n.d.)

<https://www.interpol.int/News-and-Events/News/2026/New-INTERPOL-report-highlights-escalating-cyber-threats-across-Asia-and-South-Pacific>

[54]. INTERPOL — Cybercrime Collaboration Services

Cybercrime Collaboration Services. (n.d.)

<https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services>