

Organized Crime in the Age of Modern Technology: Real-World Stakes and Prospects for Counteraction

الجريمة المنظمة في ظل التكنولوجيا الحديثة: رهانات الواقع وآفاق المكافحة

MENTALECHETA Chafik*

Faculty of Law and Political Science, University of Blida 02

c.mentalecheta@univ-blida2.dz

Date of Submission 02-04-2026 Date of Final Acceptance 22-05-2026 Date of Publication June 2026

Abstract:

Modern technology has facilitated integration and connection among individuals across borders, where digital technology has broken geographical and temporal boundaries. Conversely, the latter has directly affected transnational organized crime by turning cyberspace or the digital environment into a virtual arena for such crimes. This change has imposed challenges and obstacles of a digital, international, legal, and political nature on efforts to combat organized crime in its various forms, which target not just a single state but multiple states, thereby necessitating international solidarity and cooperation to confront this type of crime.

Keywords: modern technology, organized crime, geographical borders, the virtual arena of crime

ملخص:

لقد ساعدت التكنولوجيا الحديثة على الاندماج والارتباط بين الأفراد عبر الحدود، أين قامت التقنية الرقمية بكسر الحدود الجغرافية والزمنية، في المقابل أثرت هاته الأخيرة على الجريمة المنظمة العابرة الحدود بشكل مباشر بجعل الفضاء الرقمي أو البيئة الرقمية كمسرح افتراضي لهاته الجريمة، هذا التغير فرض تحديات وعقبات ذات طابع رقمي ودولي وقانوني وسياسي اتجاه جهود مكافحة الجريمة المنظمة بمختلف أشكالها التي تستهدف ليس دولة واحدة فحسب، وإنما أكثر من دولة، مما يستدعي ضرورة تكافل وتعاون دولي في مواجهة هذا النوع من الجريمة.

الكلمات المفتاحية: التكنولوجيا الحديثة، الجريمة المنظمة، الحدود الجغرافية، المسرح الافتراضي للجريمة

* Corresponding Author: MENTALECHETA Chafik

Introduction:

The internet and social media have become increasingly popular across different professional groups. With the growing digital revolution and the spread of media and communication technologies, the features of organized crime have changed radically in terms of planning, application, and execution. Virtual platforms have become a primary means for coordinating and connecting ideas and elements of crime among members of criminal groups behind digital screens that transcend geographic borders. This has made the digital environment a stage for transnational organized crime in new forms and patterns that rely on hiding identities and turning illicit proceeds into legitimate ones through clever use of cryptocurrencies. It has also made the transformation of organized crime more complex for law enforcement agencies in the context of strengthening countermeasures.

The importance of this study lies in analyzing its elements, starting from the relationship between transnational organized crime and technological development or globalization. Organized criminal groups now exploit technological advancement to serve their interests, which has led to the emergence of new patterns that have changed the nature of organized crime as defined in the international convention, affecting existing methods and efforts to combat it.

The primary objective of this paper is to provide multi-faceted practical insights into organized crime in light of technological development, with the aim of formulating preventive and deterrent policies based on smart technology, and others founded on international legislative frameworks that cut off criminal group members across and behind borders—particularly their exploitation of legal and judicial loopholes in international cooperation as well as the expansion of the digital space and its use in criminal activities.

This topic raises many questions that can be summarized in the research problem regarding the relationship between smart technology and organized crime and how they affect one another—especially concerning the newly developed patterns and methods of organized crime—and how to confront the challenges and stakes of the digital future for this crime amid sufficiency and international legislative gaps.

This study will employ an interweaving of different scientific research methodologies, including description, analysis, and inference, starting with defining the study's contours and clarifying how modern technology affects the particularities of transnational organized crime; analyzing its new patterns and methods and how criminal group members exploit digital technology; and analyzing the most important current and future problems and challenges resulting from technological development in relation to organized crime, so that we can identify the main gaps and try to address them by proposing a set of solutions.

Answering this problem requires a twofold plan based on two main axes that address the reality of transnational organized crime in light of the changes of the modern era, and the reality of transnational organized crime in this era's changes between the present and the future.

First: The reality of transnational organized crime in light of modern-era changes

Transnational organized crime is considered one of the most dangerous crimes threatening national, economic, cyber, legal, and judicial security in various respects, because it encompasses a set of offenses that occur between two or more states. This requires clarifying the concept of organized crime to define its contours in light of international developments and technological advances, as well as assessing the impact of modern technology on the patterns of transnational organized crime.

01_ Defining the concept of organized crime to set its contours in light of international developments

Defining any crime is the primary key to clarifying the study's contours. However, this definition alone is not sufficient for organized crime; it is necessary to specify its characteristics according to what international conventions require and the extent of their compatibility with modern developments and the evolving patterns of criminal conduct amid continuous technological advancement. This will be detailed in this section.

A. Definition of transnational organized crime

Interpol described transnational organized crime as an organization or persons linked together with the aim of engaging in continuous unlawful activity seeking to achieve interests that transcend national borders. This definition, however, was not endorsed by some countries such as Spain, Germany, and Italy because it did not include the group's structural organization, which is considered a principal element¹. Among definitions provided by Western jurists, Pella defined it from the perspective of international crime as an act or omission accompanied by a penalty proclaimed and executed in the name of the international community, while Glasser described it as a breach of international law norms that negatively affects the rules protected by that law, with legal recognition of the act as a crime and the actor's liability to punishment².

In other words, organized crime represents any violation of international law, whether criminalized under national law or recognized as such, if committed by an individual who retains freedom of choice, making them morally responsible for harming individuals or the international community at the request, encouragement, or acquiescence of a state, and whose criminal punishment is possible under the provisions of that law³.

Some German scholars defined organized crime by outlining its core characteristics, which include recourse to violence, skill and professionalism in committing offenses, use of modern technology, as well as bribery and the transnational nature of the crime, with financial profit being the primary objective of the criminal group⁴. Within international efforts, Interpol defined it as a group of persons who commit unlawful acts continuously for the purpose of making profits, even if their activities cross national borders⁵.

This definition emphasizes certain characteristics of organized crime—particularly continuity, profit-seeking, and transnational scope—but overlooks many other features; therefore Interpol's definition of transnational organized crime remains insufficient for fully delineating the crime.

The United Nations, in Article 2(a) of the United Nations Convention against Transnational Organized Crime, defined it as a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offenses established in the Convention, in order to obtain, directly or indirectly, a financial or other material benefit⁶.

It is noticeable that the UN definition, like many other definitions of transnational organized crime, omits some characteristics and includes others. Thus, transnational organized crime can be described as a set of criminal acts that violate international criminal law, carried out by a group of persons operating across different regions of states around the world who are united by a criminal project aimed at obtaining profit, whether directly or indirectly. In the context of technological development, it can be said that these are the same acts but refined with a digital electronic character, exploiting modern and advanced technology in their activities—such as money laundering, trading in virtual currencies, and digital piracy—which facilitates their evasion of legal, judicial, and security oversight in the digital space of different states.

B. Its characteristics

The European Union provides a general definition of organized crime, regardless of its type or extent, and this definition identifies eleven characteristics of organized crime, including⁷:

- International cooperation as both an element and an obstacle to confronting it.
- Cooperation among more than two persons.
- Each member undertaking a specific task.
- Continuity of activity for a long or indefinite period.
- Use of a strict form of organizational control.
- Suspected commission of serious crimes by the organization.
- Operation at the international level.
- Use of violence or terrorist methods.
- Reliance on dubious and unlawful commercial means.
- Resorting to money laundering.
- Practicing deception or exerting influence on political and judicial authorities based on the organization's underlying structures.
- Pursuit of profit and power.

From this definition it is clear that these characteristics do not appear in ordinary crimes, especially with the wave of digital transformation. Although not all of these characteristics may be present in every case of organized crime, the description of organized crime must apply to the criminal act, particularly in light of the growing implications of artificial intelligence and the spread of digital information, including identity concealment, use of encrypted digital currencies, adoption of the latest advanced digital technologies, exploitation of legal gaps related to the technological field and benefiting from conflicts of law, rapid spread through unlicensed digital platforms such as electronic black markets, and resorting to intelligent algorithms to manipulate data in order to ensure continued concealment from international security authorities.

02_ The impact of modern technology on patterns of transnational organized crime

Modern technology and the digital revolution have produced a radical change in criminology in general, whether a crime is committed domestically or externally. The latter have directly affected organized crime through the spread of digital communication means and the development of electronic infrastructures that are no longer mere channels for interpersonal communication and knowledge exchange, but have become an integrated criminal working environment among members of criminal groups from different countries. This environment enables them to plan and coordinate on a global scale quickly without geographic or security barriers, which has changed the nature and forms of organized crime.

A. The relationship between technology and organized crime

With the rapid spread of digital technology and its availability to criminals, organized crime has made the digital environment the meeting place for one or more groups from different countries around the world. A reciprocal relationship of influence has emerged between organized crime and modern technology, reflecting a changed cross-border criminal landscape.

- Impact and mutual influence

Technological development has strengthened the integration and interconnection of states and societies, especially with the advent of the Internet and social media, which led to the rise of large multinational corporations, liberalization of international trade, and removal of barriers to capital flows and global investment. Conversely, with the growing wave of technological advancement, satellites and the global information network have made the world appear as a single globe behind one digital screen, facilitating the rapid movement of information, money, and people. The combination of these conditions in developing countries creates a suitable environment for the growth of money-laundering, illicit drug trafficking, terrorism, corruption, and other forms of transnational organized crime—particularly corruption, which has become international with the globalization of markets. This has led to the internationalization of destructive illegal activities that harm national economies and are closely linked to the abuse of power and political and economic privileges, which represents one of the most dangerous effects of organized crime⁸.

In other words, organized crime, amid modern technological developments, has added a negative dimension to globalization, producing severe economic and social impacts on developing countries, where corruption has become the criminal face that best expresses organized crime. Corrupt money is treated by criminal groups as a successful type of investment and is circulated in the virtual environment digitally and in encrypted form, which increases the likelihood of their criminal success and reduces the risk of oversight, prosecution, or even arrest. Meanwhile, natural borders between states have become blurred or nearly nonexistent, facilitating the rapid spread and ease of committing this type of crime: the crime can be planned in one country, executed in another, and its effects may appear in a third⁹.

- Compatibility with the international network

Crime is directly linked to technological development; the essential characteristics of the Internet as a cross-border network align with transnational criminal activity. This relationship seeks to maximize profits while challenging risks in both the virtual world and the real world, making the activity a matter of judicial concern. When authorities try to monitor this world, they face broad jurisdictional boundaries, differing digital sovereignties, and varying areas of authority, which can make investigations slow or even impossible in some cases. The Internet offers diverse opportunities to carry out multiple types of transnational criminal operations, especially digital fraud, digital marketplaces of illicit goods, and infringements related to intellectual property¹⁰.

This relationship is evident in several ways:

- Development of criminal methods: the digital environment offers new means to commit old crimes in a cross-border digital form, such as fraud and digital extortion.
- Identity concealment: using the Internet without identifying the user is an ideal method for carrying out organized criminal activities across different countries and times. Secrecy is a core element of their strategy and organizational structure, intended to hide the trace of transactions they carry out to achieve their primary goal—financial gain.
- Increased opportunities relative to technological risks: with growing manipulation of stock prices and digital currencies, losses amounting to millions of dollars annually occur for investors. For active members of organized groups, these losses represent real opportunities to commit transnational crimes related to the digital space, especially as attention shifts to financial and informational crimes such as disrupting communication systems and destroying data.

- Circumventing legal systems: transnational crimes linked to cybercrime create zones of digital fraud and deception that lack adequate laws to combat information crimes, enabling criminals to exploit these legal gaps to their advantage.

B. Forms of organized crime in the world of modern technology

Transnational organized crime takes diverse forms under modern technology; these include cyberhacking and manipulation of illicit funds, where systems are breached to seize sensitive data or demand ransoms via digital platforms. They also include various illegal trades such as smuggling, drug- and arms-trafficking, and online fraud and scams. Other criminal patterns arise from exploiting legal loopholes, such as using personal data for identity theft, terrorist activities financed through encrypted digital platforms, illegal gambling promoted online, and phishing aimed at stealing individuals' personal information. These crimes are linked by a common characteristic: they complicate countermeasures due to their international nature and ties to technological developments. Among the most important of these forms are¹¹:

• Drug trafficking through international networks

Drug trafficking is one of the most dangerous and widespread crimes in the world; it threatens community security and negatively affects national economies. The Arab region acts as a transit hub for this activity toward Europe and Asia and also serves as a consumer market for this illicit trade. Security reports indicate that the region has begun producing this legally prohibited substance. The nature of this organized crime varies from country to country according to social and legal conditions and the level of technological development reached, especially given technological advances and the emergence of so- called “digital drugs,” or narcotic music tracks.

• Cybercrime

Cybercrime has developed markedly with advances in modern technology; it includes hacking, theft of personal information and its use in blackmail, and various offenses committed against systems or the data within them. Whatever their form, these crimes represent a threat to states' national sovereignty, calling for strengthened efforts by security agencies to confront them. The rise of this pattern of organized crime is primarily linked to digitization and technological progress.

• Illicit arms trade via the Internet

The illicit arms trade has increased in recent years, coinciding with the security breakdowns witnessed in some Arab countries in particular. This activity overlaps with terrorist groups that benefit from organized-crime services to advance their agendas, especially with the emergence of artificial intelligence and advanced technologies that have facilitated illicit deals in this field. This increases threats to state security and international peace and security, thereby multiplying the danger of organized crime.

• Smuggling crimes in the digital environment

The digital environment has become a main venue for various crimes, as smuggling activity thrives in the physical world, particularly in border areas, and includes smuggling of many goods such as foodstuffs, medicines, and energy supplies. This activity is linked to the living and social conditions of populations in those areas. With the increasing emergence of smart technologies, the financing, coordination, and marketing of smuggled products and goods has become easily conducted in the digital environment, especially with the appearance of online platforms and what is known as cyber smuggling.

• Human trafficking exploiting digital transformation

Human-rights organizations' reports indicate that human trafficking is widespread globally and particularly in the Arab region, both its African and Asian parts. This activity exploits environmental and economic conditions: the region is a transit point for waves of irregular migration from areas of conflict and poverty, and migrants are often exploited in inhumane ways, in addition to activities such as prostitution and organ trafficking, which are unlawful crimes. Active accounts on social media exploit this gap to promote exploitative and opportunistic offers to attract certain vulnerable groups and take advantage of marginalized people, exploiting them in trafficking operations either as humans or for human organs.

• Money laundering

National and global security face major challenges in combating money laundering due to weak legal frameworks and loopholes exploited by organized-crime networks. Money-laundering operations result from illicit activities such as drug trafficking and irregular migration and include smuggling of hard currency, particularly amid technological developments and the emergence of digital currencies.

It facilitates technological development for perpetrators of organized crime in its various forms from different aspects, as the use of modern technological techniques has become a basic pillar in carrying out and concealing criminal activity; for example, we use digital encryption applications in money laundering and drug trafficking operations to coordinate smuggling and hide identities. Electronic black markets are the new marketplace for legitimizing illicit funds, while social media platforms are exploited to lure victims and coordinate their transport, especially in human trafficking. Cryptocurrencies provide hard-to-trace transfer channels for money laundering and cybercrime (hacking, data theft, extortion), which expand due to weak digital protection and the lack of effective countermeasures against this type of crime.

Second: Confronting the danger of organized crime between enforcement efforts and the challenges of digitization

Given the severe impact of modern technological developments on organized crime, it has become necessary to analyze international enforcement efforts against this crime and assess their compatibility with the effects of the digital transformation wave. The United Nations has contributed significantly in this field despite the existence of major challenges and obstacles directly related to the nature of the crime and the specificity of technological development.

01_ The trend toward developing enforcement mechanisms in line with the requirements of the digital transformation

International conventions have defined a set of international efforts, alongside organizations including Interpol (the International Criminal Police Organization). Moreover, keeping pace with developments in contemporary criminal policy involves using modern technological methods in research and investigation of organized crime, and emphasizes cooperation in applying and executing the surrender of criminals. This will be detailed below.

A_ Between prevention and punishment

Prevention is considered a stage prior to punishment. Within the framework of combating organized crime, the United Nations Convention has adopted a set of measures and mechanisms aimed at combating transnational criminal activities and disrupting the ability of criminal organizations to carry them out regardless of their severity. These measures are not based on a single procedure; rather, they vary between those applied domestically and those exchanged cooperatively among member states of the Convention, between prevention and punishment in confronting patterns of organized crime at the global level. The most important of these methods are as follows:

• Oversight and supervision of institutions where criminal activity may occur

Among the basic measures that states undertake within the framework of the Convention is the establishment of internal supervisory systems concerned with oversight of banks and non-banking financial institutions. This oversight also extends to any entities exposed to the risk of money laundering. These systems aim to track capital movements and detect all forms of money laundering by tightening Know Your Customer (KYC) requirements, record-keeping, and reporting suspicious transactions that warrant investigation into the sources of funds¹².

This measure allows for an effective supervisory system in confronting transnational crime by reporting unusual transactions whose values or characteristics are inconsistent with the nature of the client's activity or market logic and that do not appear to have an apparent economic purpose or legal justification. It should be emphasized that this requires broad cooperation and information exchange at national and international levels. Hence, states establish national financial intelligence units to collect, analyze, and disseminate information before the crime occurs¹³.

For supervisory purposes, effective measures are also taken to monitor the movement of cash and negotiable instruments across borders, while establishing safeguards that protect the freedom of legitimate capital movement. For example, individuals and institutions may be required to report large cross-border cash transfers or negotiable instruments suspected of being illicit. When establishing their supervisory and oversight systems, states should base them on regional and international initiatives and standards adopted to combat money laundering, so that they adopt measures that impede this crime without infringing on states' domestic systems¹⁴.

• Cooperation with law enforcement agencies

It refers to the cooperation provided by persons involved in organized criminal group offenses with the authorities responsible for combating these crimes. This includes, in particular, a number of instructions and safeguards that facilitate such cooperation, which include the following¹⁵:

- Providing information that assists authorities in investigation and proof regarding the identities of individuals involved in criminal groups or the nature of those groups' activities or their organizational composition and structure.
- Disclosing internal and external relationships that link the criminal group with other groups, whether domestically or across borders.
- Supplying information about crimes that have been committed or that may be committed by these groups.
- Providing anything that contributes to stripping these groups of their resources and thwarting the sources of financing for their criminal activities.

This type of cooperation is more effective than before, especially given the growth of modern technology, because it can reveal and report a large number of crimes electronically, particularly when taking into account the circumstances surrounding persons involved in organized crime, which may be social or the result of coercion. Nevertheless, such cooperation requires providing protection for these reporting persons and granting incentives that encourage them to assist the competent state authorities in ways that do not conflict with the objectives of the Convention. This includes mitigating penalties, providing protection and care, as well as protecting whistleblowers at the legal and judicial levels¹⁶.

• International technical assistance

When discussing the fight against organized crime, we are not dealing with a single crime but a set of crimes for which sufficient technical assistance must be provided to states to implement the Convention's provisions to achieve this fight, through regular donations from donor states in coordination with the United Nations, and the possibility of allocating a percentage of crime proceeds or confiscated property according to available capacities. States and financial institutions should also be encouraged to provide training programs and to supply modern means and technologies based on advanced technology and artificial intelligence to developing countries to help them achieve the Convention's objectives accurately and systematically¹⁷.

• International judicial prosecution

Judicial prosecution is considered a fundamental deterrent measure to prevent crime regardless of its type and embodies international cooperation at the judicial level. The Convention affirmed the necessity of subjecting the offenses it lists — including those in the supplementary protocols — to penalties that reflect their gravity, including liability for both natural and legal persons pursuant to paragraphs 2 and 4 of Article 10 of the Convention. This is to ensure maximum effectiveness of law enforcement measures while observing the goal of deterrence. Judicial prosecution concludes with the trial of persons involved in the offenses under consideration while guaranteeing the right to defense. Conversely, to prevent impunity, the Convention obliged states to take necessary national measures to ensure the accused appear before subsequent criminal proceedings if released during trial or before appeal, to avoid exploitation of safeguards that allow avoidance of detention¹⁸.

• Cooperation in the application and execution of extradition

First, this procedure can be described as the system by which a state surrenders a person located in its territory to another state at that state's request for trial for an offense punishable under its law or for the execution of a sentence imposed by one of its courts. According to Interpol's media bulletin, it is defined as the requested state delivering a person present in its territory to another state that requests them either for trial on an alleged offense or for the execution of a sentence. Article 1 of the Model Treaty on Extradition (General Assembly resolution 45/116) defines extradition as the set of legal measures by which a state surrenders an accused or convicted person to another state so that they may be tried there or the sentence imposed against them may be executed. The Convention against Transnational Organized Crime sets out a range of conditions and procedures to be followed in the extradition system to ensure verification and cooperation among states¹⁹.

• Use of modern technical methods in investigation and inquiry into organized crime

Modern criminal systems, by virtue of some international conventions, have tended to expand exceptional systems to confront the gravity of certain crimes, including transnational organized crime—particularly when committed in the digital environment—which has affected the course of ordinary criminal procedures through measures aimed at restricting procedural guarantees provided for in constitutions and criminal procedure law. For example, Algerian legislators sought to keep pace with these international developments in combating organized crime in line with ratified charters and international conventions. They enacted successive amendments to the provisions of the Code of Criminal Procedure from 2004 up to Law No. 25_14, which reorganized criminal procedural provisions in general. This included introducing new procedural rules that expand the jurisdiction of the judiciary and strengthen the powers of judicial police officers, alongside adopting new methods and mechanisms for inquiry and investigation into these crimes that sometimes departed from general procedural rules. These special investigative techniques include²⁰:

- Intercepting correspondence and recording voices

- Photography capture
- Electronic surveillance
- Electronic searches

B_ At the level of international organizations

International organizations have played a major role in strengthening efforts to combat transnational organized crime in its various forms, foremost among them Interpol and European and African organizations, as well as cybercrime complaint centers. This reflects how enforcement efforts have kept pace with and been shaped by modernization and continuous technological development, expanding the scope of those efforts in line with contemporary interactions between technology and organized crime.

• International police efforts — Interpol

Interpol plays an important role in enabling police forces around the world to make the environment safer. It provides the tools and services these forces need to perform their tasks effectively while keeping pace with evolving forms of transnational organized crime. The International Criminal Police Organization established a specialized branch on organized crime attached to the General Secretariat to conduct related studies, and it created a database of persons involved in illicit activities. It also defined standards for the concept of organized crime at the Fifth Conference on Transnational Organized Crime held in Lyon, France, in 1996. In addition, Interpol established a Criminal Analysis Unit where important information about criminal organizations is extracted and classified to be made available to police and Interpol member states²¹.

To strengthen the organization's infrastructure, improve its operating model, and promote its role in leading police work and supporting law enforcement efforts with a long-term vision, Interpol relies on several core tools that facilitate its work in combating patterns of organized crime in step with the digital transformation. Examples include:

- Databases

Key databases used by Interpol include²²:

- **Child Sexual Exploitation Image Database:** This database is an intelligence and investigative tool that allows specialist investigators to exchange information about child sexual abuse cases, especially in the digital space. Thanks to image- and video-matching programs, it can instantly link victims, perpetrators, and locations. The database enables investigators from more than 68 countries to share data internationally; it contains over 27 million images and video clips and has helped identify 23,564 victims worldwide.

- **Stolen and Lost Travel Documents (SLTD) database:** This contains information on reported stolen, lost, revoked, or forged passports and identity documents. It enables law enforcement to verify document validity in seconds. For example, in 2021 it processed around 17 billion checks resulting in 146,000 positive matches. Interpol developed the "Checkit" app to help detect use of stolen documents before people reach airports and border crossings, contributing to the apprehension of terrorists and criminals and enhancing efforts to combat human trafficking as a transnational crime.

- **DNA database:** Established in 2002, it now contains hundreds of thousands of DNA profiles (supplied by about 48 member countries), allowing police to compare samples taken from perpetrators, crime scenes, missing persons, or unidentified remains and obtain results within minutes. The database has helped investigators link offenders to various crimes—particularly rape, murder, and armed robbery—and identify missing persons when remains are found.

- Global secure communications network

Interpol operates a global police support and secure communications system known as "24/7" that connects law enforcement agencies in member countries, enabling authorized users to exchange crucial police data and access the organization's databases and services around the clock. Through this network, Interpol provides advanced analytical and database services to help prevent crime, locate and apprehend fugitives and transnational criminals, and determine their whereabouts²³.

- Interpol notices

The organization issues several notices at the request of a member country to combat organized crime and apprehend wanted persons worldwide. Important notices include²⁴:

- Red Notice: A request to law enforcement worldwide to locate and provisionally arrest a person pending extradition, based on an arrest warrant or court order issued by the requesting state's judicial authority.
- Yellow Notice: A global alert about a missing person, published to help locate missing persons—especially minors—or to identify persons unable to identify themselves.
- Blue Notice: Used to collect information about a person's identity or activities in relation to a criminal investigation.
- Green Notice: Issued to warn of criminal activities by a person who may pose a threat to public safety and who might commit similar offenses in other countries.
- Black Notice: Used to request information on unidentified bodies.
- Orange Notice: Added in 2004 to warn of an event, person, or modus operandi that poses an imminent threat to people or property.

Interpol's vision is to establish a world in which the law is enforced through essential communication among international police agencies, keeping pace with the evolution of transnational crime to facilitate information exchange, coordinate operations, and arrest as many criminals as possible in light of technological advances and increasingly tech-enabled criminal methods.

In practice, some of the most significant extraditions facilitated by Interpol include cases reported to the Interpol Secretariat by Estonia. In 2009 and 2010 the United States submitted three extradition requests concerning three suspects alleged to belong to criminal organizations that committed electronic fraud targeting Egypt. Those requests were legally based on the United Nations Convention against Transnational Organized Crime and the bilateral extradition treaty between Estonia and the United States (2006), as well as the Council of Europe Convention on Cybercrime. Estonia extradited the three individuals to the United States, and their cases remain under investigation²⁵.

· European organizations' efforts

Europol established the European Cybercrime Centre in 2013 to strengthen law enforcement responses within the European Union to cybercrime as a form of organized crime. The Eurojust network was established in February 2002 and began operating in April 2003 with the aim of judicial coordination among the EU member states. In Budapest in 2001, the Convention on Cybercrime was concluded with the participation of 26 countries as well as Canada, Japan, South Africa, and the United States; this was the first international treaty to address offenses committed against or by means of computer networks, and it was opened for accession by interested states with the aim of expanding the scope of combating organized crime. Likewise, the Council of Europe established in Luxembourg in 1991 a European police unit that acts as a liaison among police forces in the Union's countries to pursue perpetrators of cross-border crimes²⁶.

• Efforts of African organizations

The African Union adopted a Convention on Cybersecurity and Personal Data Protection at its 23rd Ordinary Session held in Malabo (Equatorial Guinea) on 27 June 2014. Its primary objective is to strengthen legislative and regulatory frameworks for information and communication technologies among member states, especially the security rules necessary to create a trusted digital space for electronic transactions, protect personal data, and combat cybercrime. The African legislator divided the content of the Convention into four main groups²⁷:

- The first group concerns attacks on computer systems
- The second group relates to crimes based on personal data
- The third group addresses content-related offenses
- The fourth group concerns offenses related to securing electronic communications

Accordingly, specialized institutions and facilities operate under these headings. The idea of creating “Afripol” also crystallized during the Oran conference in Algeria in 2013, where this body was tasked with enhancing analytical capacity to assess criminal threats and develop appropriate responses, in addition to providing technical assistance in the field of cybercrime and supporting peacekeeping operations.

• Internet Crime Complaint Center

This center was established in the United States in 1998 with the advent of commercial and financial activities on the Internet, at the FBI’s initiative to provide a dedicated body to receive cybercrime complaints and distinguish them from other crimes. The first operational center opened in 1999 under the name “Internet Fraud Complaint Center,” then it was renamed in 2002 to the “Internet Crime Complaint Center” after clarifying its scope of competence so that it expanded from handling simple fraud to emergent criminal activities on the network. The IC3 website allows anyone anywhere in the world to file complaints, and the center cooperates with international organizations and agencies specialized in combating Internet crimes. The center also coordinates with the Economic and Financial Crimes Commission in Nigeria and the Canadian Anti-Fraud Centre, and it cooperates with many countries including Australia and the United Kingdom²⁸.

02_ Obstacles to achieving comprehensive combating of organized crime in the era of modernization and development

The challenges and obstacles to combating transnational organized crime are numerous and occur at different levels. This is natural given the diversity of criminal patterns that constitute organized crime, and these challenges vary according to each criminal pattern, especially with the growing implications and dynamics of modern technology and its alteration of the ways crimes are committed and executed. Among the most important of these obstacles are those of legal, judicial, digital, and even political dimensions, the most prominent of which is:

A_ The principle of territoriality of criminal laws

It is self-evident that the state alone has the authority to enact its legislation and apply it to crimes that occur within its political borders in accordance with its social circumstances and economic interests; no other state may share those powers. Criminal law therefore embodies manifestations of state sovereignty, and it is founded on the principle of territoriality, which was later subject to a significant development in the form of an extension of the scope of national law to include crimes committed outside the state’s territory—sometimes under the nationality principle or the protective principle as exceptions to territoriality and to facilitate the proper conduct of proceedings in organized

or international crime in general. However, this development has not kept pace with the accelerated evolution of crimes, especially those that make use of modern information technology. Although criminal law is primarily concerned with combating crime within the state's territory, many offences—including cross-border financial crimes and destructive threats to life such as drugs, chemical weapons, and other forms of organized crime—are rapidly expanding in an environment characterized by free trade and investment and taking advantage of technological development²⁹.

Here the principle of territoriality of criminal law, in the context of modern technological development, raises fundamental challenges to combating transnational organized crime, particularly with regard to speed, application, and enforcement of a state's law. International cooperation mechanisms, which are themselves slow, hinder rapid access to evidence—especially digital evidence that is ephemeral. There are also restrictions on direct access to digital evidence between two or more states across geographic borders: authorities cannot act on servers or accounts located in other jurisdictions without the express and direct consent of the public prosecutor or competent authorities. In addition, conflicts and contradictions exist in certain legislative matters and incompatibilities among legal provisions—particularly concerning privacy protection, fundamental rights, and digital sovereignty—which restrict the exchange of information and the use of surveillance technologies. This enables cross-border offenders to exploit these technical and legal gaps to escape and conceal traces of their crimes from the competent authorities.

B_ The problem of recognition of foreign judgments in terms of probative effect and enforcement

The general rule is that each state recognizes only the judgments of its own criminal law and gives effect to the decisions of its courts based on the principle of territorial and judicial sovereignty. Accordingly, the courts of each state do not grant probative value to judgments issued by other states, because a criminal judgment is considered an expression of state sovereignty. But every rule has exceptions: a foreign criminal judgment may exceptionally be enforced when this does not conflict with the principle of international sovereignty and does not contravene public order and public morals; enforcement occurs only with the consent and choice of the state concerned. Duties arising from the protection of humanity also allow that criminal punishment may, in some cases, transcend territorial limits, as is the case with transnational organized crime, particularly given the growing implications of artificial intelligence and modern technology. Despite the importance of foreign criminal judgments, their practical enforcement remains an obstacle to confronting transnational organized crime; sometimes circumstances call for imposing a harsher penalty on the defendant if tried before national courts, so a foreign acquittal or a foreign judgment that reduces sentence may not be recognized if local circumstances require a stricter trial³⁰.

On the other hand, most national legislations hesitate to acknowledge the positive effect of foreign criminal judgments, which constitutes an impediment to effective combat against transnational organized crime. An example is Algerian legislation, which does not grant such judgments enforceable force within its territory except where a cooperation agreement exists between Algeria and the issuing state. Referring to the United Nations Convention against Transnational Organized Crime, that instrument did not give priority to the probative effect of foreign criminal judgments; it addressed the matter in paragraph 12 of article 16 concerning the extradition of offenders to avoid the adverse effects of refusal to extradite. Hence, there is a need to accord greater importance to this issue and to clarify means of international cooperation for enforcing foreign criminal judgments³¹.

C_ Negative stances of states toward treaties on international judicial and criminal cooperation

An international convention serves as a guiding and contractual instrument for member states in applying and implementing the legal obligations it contains. Currently, international criminal policy in many areas is largely limited to coordinating procedures among states with divergent criminal

systems, because this approach aims to develop security and judicial cooperation while respecting each state's particularities according to contemporary criminal policy developments. Nevertheless, some states adopt negative stances toward establishing an integrated international criminal system out of concern that it would impose rules and legal concepts grounded in philosophical or cultural foundations that do not align with their social and cultural realities. Thus, adopting a unified international criminal system could lead to a form of cultural homogenization that disregards societies' cultural diversity, which motivates states to reserve or decline to accept international texts or obligations that may conflict with their legal and social identity³².

This is particularly true when digital sovereignty is at stake amid technological development, where states' reluctance prevents them from signing agreements; this limits cooperation in confronting transnational organized crime in the information age and reduces the effectiveness of international cooperation mechanisms. These negative stances weaken the international community's capacity to respond promptly to real crimes carried out under the guise of organized crime amid the challenges of digitization and contemporary technology, leading to:

- Weakening cooperation among international institutions: when some states withhold from an agreement, this amounts to rejecting the strengthening of international cooperation mechanisms, which impedes coordination with technology companies and slows judicial authorities' ability to obtain numerous reliable pieces of evidence necessary to investigate cross-border crime.
- Imposing constraints on immediate access to material and digital evidence across virtual borders: digital sovereignty emerges as a difficult-to-overcome obstacle, increasing procedural coordination difficulties and resulting in the loss of vast amounts of evidentiary material that would otherwise streamline procedures.
- Reducing the scope of international cooperation: hesitation or refusal to join international cooperation mechanisms manifests as a refusal to cooperate in combating transnational organized crime, creating geographic and digital gaps that usually benefit members of criminal networks.

D_ The problem of the special nature of transnational organized crime

Organized crime is characterized by particular subtleties: the difficulty of detecting and combating it stems from its nature. For example, cybercrime, being transnational, raises difficulties in identifying the state with jurisdiction and in determining the applicable law, in addition to procedural problems in criminal prosecution. Reaching the truth in such cases requires reliance on advanced technical expertise, since cybercrime does not respect time or place; the temporal, spatial, and legal dimensions play a major role in dispersing investigative efforts and international coordination. This type of crime does not confine itself to a single state but targets several states simultaneously, and the whole world can become the stage of the crime where the offender can act from any location at any time³³.

Conclusion:

In conclusion, the subject of organized crime in general is among the most important topics requiring study and detailed analysis, especially regarding international cooperation in the era of modern technology and the growing artificial intelligence revolution. Organized crime has become a more complex and dynamic phenomenon in terms of planning, execution, and implementation, making the digital environment a virtual stage for newly emerging transnational criminal patterns, foremost among them money laundering, virtual currency transactions, cyber-enabled crimes, and the offences covered by the Convention. It is noticeable that modern technology has expanded the operational space of these crimes across borders and behind a digital screen, giving rise to particular challenges and obstacles despite efforts to combat them and to adapt those efforts to contemporary developments.

Study findings

This study produced a number of findings, the most important of which are:

- Increased technical and scientific complexity in combating organized crimes with respect to collecting evidence, accessing it, and apprehending perpetrators.
- Transnational organized crimes have adopted digitally mediated forms that overlap several criminal characterizations, especially regarding the financial aspect between money laundering and virtual currency transactions.
- Weak international cooperation amid rapid technological development makes it difficult to precisely classify and investigate organized crime, which hinders judicial cooperation and allows members of criminal networks to exploit legal gaps and practical shortcomings.
- Reliance on traditional combat mechanisms is insufficient to confront transnational organized crime; it is necessary to keep pace with modern technological developments.

Study recommendations

- The situation requires adopting a hybrid international strategy combining traditional and modern elements, flexible international legislation, and advanced technical capabilities in the field of international cooperation to combat transnational organized crime in all its forms.
- Update and develop international legal frameworks, conventions, and treaties related to organized crime to incorporate modern technology in terms of criminalization and in combating it, so as to cover all digital acts that cross territorial borders in a virtual crime theatre.
- It is essential to make use of modern technological tools and establish flexible mechanisms adaptable to new transnational criminal developments, such as creating digital forums to exchange political and legal dialogue on practices that violate rules and international law, supported by digital protection against cyberattacks.
- It is advisable to establish international specialized units within law enforcement agencies staffed by experts in international criminal law and international criminal procedure and in cybersecurity. These units should analyze big data on international criminals and rely on advanced techniques to analyze and predict network activity, with shared digital criminal databases among member states while respecting their sovereignty.
- Strengthen international cooperation by initiating or calling for international agreements on combating transnational organized crime, with emphasis on the rapid and immediate exchange of information to ensure effective pursuit of transnational criminal networks.

Bibliography:**A_ Books**

- Ben Maki Najat, Criminal Policy to Combat Computer Crimes, Dar Al-Khaldounia, Al-Qubba Al-Qadima, Algeria, 2017.
- Hoda Hamed Qashqoush, Organized Crime: Substantive and Criminal Rules and International Cooperation, Dar Al-Nahda Al-Arabiya, Cairo, 2000.
- Jihad Muhammad Al-Brizat, Organized Crime: An Analytical Study, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2010.

- Manasra Yusuf, Crimes Affecting Automated Data Processing Systems: Their Nature, Forms, International Efforts to Combat Them, Comparative Study, Dar Al-Khaldounia, Al-Qubba Al-Qadima, Algeria, 2018.
- Nabil Saqr, Qamrawi Ezzedine, Organized Crime: Smuggling, Drugs and Money Laundering in Algerian Legislation, Dar Al-Huda for Printing, Algiers, 2008.
- Nadia Qasim Baydoun, Organized Crime: Corruption and Money Laundering, 2nd ed., Beirut, 2012.
- Nisreen Abdel Hamid Nabih, Transnational Organized Crime, Dar Al-Fikr Al-Jami'i, Alexandria, 2007.
- Suleiman Ahmed Ibrahim, Criminal Rules of Organized Crime and International Cooperation to Combat It, Dar Al-Kitab Al-Hadith, Cairo, 2008.

B_ Theses

- Amina Allali, Cross-border Crimes Committed Using Internet Technology, PhD thesis in Law, Faculty of Law and Political Science, Department of Law, Criminal Law specialty, University of Badji Mokhtar Annaba, 2018/2019.

C_ Articles

- Bakhouya Driss, Chergui Khadija, "Globalization of criminal legislation to confront global organized crime," African Journal of Legal and Political Studies, Vol. 01, No. 01, 2017.
- Benzaid Salima, "International Cooperation Mechanisms for the Prevention of Transnational Organized Crime," Journal of Comparative Legal Studies, Vol. 09, Issue 01, 2023.
- Gaceime Mahjoba, "INTERPOL, an international mechanism to combat transnational organized crime," Journal of Research in Law and Political Science, Vol. 09, Issue 01, 2023.
- Houcine Hayet, "The implications of technological development on organized crime and the mechanisms to combat it internationally," Journal of Legal and Political Thought, Vol. 6, Issue 1, 2022.
- Linda Mohad, "Exceptional measures to confront transnational organized crime," Department of Research, Studies, Legal and Political, Vol. 05, Issue 03, 2021.
- Mabrouk Kahi, "Organized Crime in the Arab Region: Factors of Spread, Forms of Emergence, Mechanisms of Combat," Journal of Human Sciences, Vol. 32, No. 04, 2021.
- Malika Hadjadj, Ounnoughi Nabil, "International coopération to confront transnational organized crime between the ingrédients and obstacles," Academic Journal of Legal and Political Research, Vol. 6, Issue 1, 2022.
- Mohamed-Said Bouflih, "International cooperation frameworks to address cyber threats," Journal of Applied Legal Studies, Vol. 1, No. 2, 2024.
- Salem Sharmat, "Transnational Organized Crime: Concept, Effects and Obstacles to Its Combat," Academic Journal of Legal and Political Research, Vol. 05, No. 02, 2021.
- Zakarya Semghouni, "International and Domestic Legal Mechanisms for Combating Transnational Organized Crime and Ways to Strengthen Them," Journal of Legal and Political Research, Vol. 02, Issue 15, 2020.

D_ International conventions

- United Nations Convention against Transnational Organized Crime, adopted and opened for signature, ratification and accession by General Assembly resolution 55/25 of 15 November 2000.

Citations:

¹ Hoda Hamed Qashqoush, Organized Crime : Substantive and Criminal Rules and International Cooperation, Dar Al-Nahda Al-Arabiya, Cairo, 2000., p. 6

² Amina Allali, Cross-border Crimes Committed Using Internet Technology, PhD thesis in Law, Faculty of Law and Political Science, Department of Law, Criminal Law specialty, University of Badji Mokhtar Annaba, 2018/2019 p 45

³ Nabil Saqr, Qamrawi Ezzedine, Organized Crime : Smuggling, Drugs and Money Laundering in Algerian Legislation, Dar Al-Huda for Printing, Algiers, 2008, p 09

⁴ Jihad Muhammad Al-Brizat, Organized Crime : An Analytical Study, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2010, p 10

⁵ Nadia Qasim Baydoun, Organized Crime : Corruption and Money Laundering, 2nd ed., Beirut, 2012, p 12

⁶ Article 02 United Nations Convention against Transnational Organized Crime, adopted and opened for signature, ratification and accession by General Assembly resolution 55/25 of 15 November 2000.

⁷ Malika hadjadj, Ounnoughi nabil, International coopération to confront transnational organized crime between the ingrédients and obstacles, Academic Journal of Legal and Political Research, Volume 6, Issue 1, 2022, p 433

⁸ Houcine hayet, The implications of technological development on organized crime and the mechanisms to combat it internationally, Journal of Legal and Political Thought, Volume 6, Issue 1, 2022, p 574

⁹ Ibid, p 575

¹⁰ Houcine hayet, op cit, p 575_576

¹¹ Mabrouk Kahi, « Organized Crime in the Arab Region : Factors of Spread, Forms of Emergence, Mechanisms of Combat, » Journal of Human Sciences, Vol. 32, No. 04, 2021, p 641

¹² Zakarya semghouni, International and Domestic Legal Mechanisms for Combating Transnational Organized Crime and Ways to Strengthen Them, Journal of Legal and Political Research, volume 02, issue, 15, 2020, p 201

¹³ Suleiman Ahmed Ibrahim, Criminal Rules of Organized Crime and International Cooperation to Combat It, Dar Al-Kitab Al-Hadith, Cairo, 2008, p 119

¹⁴ Nisreen Abdel Hamid Nabih, Transnational Organized Crime, Dar Al-Fikr Al-Jami'i, Alexandria, 2007, p 61

¹⁵ Article 26, paragraph 1, of the United Nations Convention against Transnational Organized Crime

¹⁶ Zakarya semghouni, OP cit, p 205_206

¹⁷ Article 20 of the United Nations Convention against Transnational Organized Crime

¹⁸ Zakarya semghouni, OP cit, p 210

¹⁹ Malika hadjadj, Ounnoughi nabil, OP cit, p 441_442

²⁰ Linda mohad, Exceptional measures to confront transnational organized crime, Department of Research, Studies, Legal and Political, volume 05, issue 03, 2021, p 180_183

²¹ Benzaid Salima, International Cooperation Mechanisms for the Prevention of Transnational Organized Crime, Journal of Comparative Legal Studies, Volume 09, Issue 01, 2023, p 694

²² Gaceime mahjoba, INTERPOL, an international mechanism to combat transnational organized crime, Journal of Research in Law and Political Science, Volume 09, Issue 01, 2023, p 349

²³ Gaceime mahjoba, OP cit, p 350

²⁴ Ibid, p 351_352

²⁵ Malika hadjadj, Ounnoughi nabil, OP cit, p 445

²⁶ Mohamed-said bouflih, International cooperation frameworks to address cyber threats, Journal of Applied Legal Studies, Volume 1, Numéro 2, 2024, p 17

²⁷ Manasra Yusuf, Crimes Affecting Automated Data Processing Systems : Their Nature, Forms, International Efforts to Combat Them, Comparative Study, Dar Al-Khaldounia, Al-Qubba Al-Qadima, Algeria, 2018, p 283

²⁸ Ben Maki Najat, Criminal Policy to Combat Computer Crimes, Dar Al-Khaldounia, Al-Qubba Al-Qadima, Algeria, 2017, p 138_142

²⁹ Bakhwiya Driss, Sharqi Khadija, Globalization of Criminal Legislation to Confront the Globalization of Organized Crime, African Journal of Legal and Political Studies, Volume 1, Issue 1, 2017, p. 53

³⁰ Malika hadjadj, Ounnoughi nabil, op cit, p 450

³¹ Ibid, p 451

³² Bakhwiya Driss, Sharqi Khadija, op cit, p. 53

³³ Salem Sharmat, Transnational Organized Crime : Its Concept, Effects, and Obstacles to Combating It, Academic Journal of Legal and Political Research, Volume 05, Issue 02, 2021, p. 531