Ashdin Publishing
Journal of Drug and Alcohol Research
Vol. 15 (2026), Article ID 236512, 06 pages
DOI: 10.4303/JDAR/236512

*Research Article*

# Legal Mechanisms for Combating Organized Crime in the Field of Illicit Drug Trafficking in Cyberspace: European Experience and Prospects for Ukraine

**Yurii Vykhodets[1*], Yurii Pavliutin[2], Hanna Teteriatnyk[3], Liudmyla Holynska[4], Volodymyr Dryshliuk[5], Natalia Kalynka[6]**

[1]*Department of Criminology and Information Technologies, National Academy of Internal Affairs, Kyiv, Ukraine*
[2]*Department of Administrative Activities of the Police, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine*
[3]*Department of Criminal Procedure and Criminology, Odesa State University of Internal Affairs, Odesa, Ukraine*
[4]*Department of Criminal Procedure and Criminology, Odesa State University of Internal Affairs, Odesa, Ukraine*
*5Director, Institute of Law and Security, Odesa State University of Internal Affairs, Odesa, Ukraine*
[5]*Odesa State University of Internal Affairs, Odesa, Ukraine*

**Address Correspondence to: Yurii Vykhodets, Email: yurii.vykhodets@cyberpolice.gov.ua*

**Received:** 15 April 2026; Manuscript No: JDAR-26-194428; **Editor assigned:** 17 April 2026; PreQC No: JDAR-26-194428 (PQ); **Reviewed:** 01 May 2026; QC No: JDAR-26-194428; **Revised:** 08 May 2026; Manuscript No: JDAR-26-194428 (R); **Published:** 15 May 2026; DOI: 10.4303/JDAR/236512



**Abstract**

**Aim:** The article examines legal mechanisms for combating organized crime in the field of illicit drug trafficking in cyberspace, taking into account modern trends in the digitalization of the drug market and European experience.

**Methods:** The methodological basis of the study is the systematic, comparative law, formal law, criminological and legal modeling methods. The European Union's approaches to combating digital drug crime are analyzed, in particular the activities of the European Union Drugs Agency (EUDA), Europol, European Cybercrime Centre (EC3) and European Union Agency for Criminal Justice Cooperation (Eurojust), as well as international mechanisms for combating transnational organized crime, cybercrime and money laundering. It has been established that effective counteraction to the digital drug business requires a combination of criminal law, criminal procedure, information, financial monitoring and international legal instruments.

**Results:** It is substantiated that the use of web resources, darknet platforms, social networks, encrypted messengers, cryptoassets and other digital tools by organized criminal groups leads to the transformation of traditional forms of illicit drug trafficking and creates new challenges for the criminal justice system. The purpose of the study is to determine the features of legal support for combating organized drug crime in cyberspace, analyze European mechanisms and formulate proposals for their adaptation in Ukraine.

**Conclusion:** The need to move from a fragmented response to individual facts of illegal drug trafficking to a comprehensive impact on the digital infrastructure of organized crime networks is proven. Directions for improving Ukrainian legislation and law enforcement practice are proposed, in particular regarding the documentation of electronic evidence, the detection and confiscation of crypto assets, blocking digital channels of illegal trafficking, strengthening interagency cooperation and the development of Ukraine's cooperation with Europol, Eurojust and other international law enforcement agencies. The feasibility of forming an integrated system for monitoring the digital drug market and a risk-based approach to detecting organized crime networks in Ukraine is substantiated.

**Keywords:** Organized crime, Drug trafficking, Cyberspace, Digital drug crime, Darknet, Cryptoassets, Electronic evidence, Cybersecurity, Europol, International cooperation

**Abbreviations:** EUDA: European Union Drugs Agency; Eurojust: European Union Agency for Criminal Justice Cooperation

## Introduction

The rapid development of digital technologies has significantly transformed the mechanisms of functioning of organized crime in the field of illicit trafficking of narcotic drugs and psychotropic substances. While the traditional model of drug crime mainly involved direct physical contact between the manufacturer, intermediary, seller and consumer, the modern illegal market is increasingly moving to cyberspace. Specialized web resources, social networks, messengers with end-to-end encryption, darknet platforms, cryptocurrencies and other digital tools that ensure a high level of anonymity of participants in criminal activity are used to organize illicit trafficking [1,2].

According to international organizations, the digitalization of illicit drug trafficking has become one of the determining factors in the transformation of the modern drug market. The use of digital platforms allows organized crime groups to search for clients, advertise drugs, coordinate the activities of participants, accept orders, conduct financial transactions and hide the proceeds of crime without the need for physical interaction between individual links of the criminal network [1].

Of particular danger is the use of crypto-assets and other digital financial instruments by organized crime groups. Such technologies can be used to complicate the establishment of the origin of funds, the identification of participants in financial transactions and the tracking of cross-border flows of income derived from illicit drug trafficking. In combination with anonymization technologies, encrypted communication channels and the distributed structure of criminal networks, this creates new challenges for criminal justice and international law enforcement cooperation [3].

European experience indicates a gradual transition from responding to individual facts of illicit drug trafficking to a comprehensive model of countering organized crime ecosystems. This model involves a combination of criminal law, criminal procedure, financial law, information and international law mechanisms. An important role in its implementation is played by Europol, the EUDA, Eurojust, the European Cybercrime centre (EC3), national law enforcement agencies and specialized financial monitoring bodies [2,4].

For Ukraine, this issue is of particular relevance due to the active use of digital technologies for the illegal distribution of drugs, the activities of online stores, telegram channels, anonymous payment systems and crypto assets. At the same time, countering such manifestations requires not only improving criminal legislation, but also the formation of a holistic legal mechanism for identifying the digital infrastructure of organized drug crime, documenting electronic evidence, blocking criminal financial flows and developing international cooperation.

The issue of illicit drug trafficking is traditionally studied within the framework of criminal law, criminology, forensics and international law. At the same time, the modern stage of development of the information society has led to the formation of a separate research area related to the digitalization of the drug market and the use of cyberspace by organized criminal groups.

Of great importance for the study are analytical materials from the United Nations Office on Drugs and Crime (UNODC), the European Drug Agency (EDA), Europol and other international institutions. The relevant documents emphasize that modern organized criminal networks use digital technologies not only as an auxiliary means of communication, but as an independent element of the infrastructure of the illegal drug market [1,2].

European research pays significant attention to the activities of online drug markets, the functioning of darknet marketplaces, the use of cryptocurrencies and encrypted communication platforms. Of particular interest is the transnational nature of digital drug crime, since servers, platform administrators, sellers, buyers, and financial intermediaries can be located in different jurisdictions [3,4].

The issue of comprehensive use of European experience to improve legal mechanisms for combating organized drug crime in Ukraine remains insufficiently researched. That is why there is a need for a systematic analysis of the relationship between criminal law, criminal procedure, cybersecurity, financial, and international countermeasures.

## Methods

The comparative legal method in the study of legal mechanisms for combating organized crime in the field of illicit drug trafficking in cyberspace has a special methodological significance, as it allows not only to compare the provisions of the legislation of Ukraine and the European Union (EU), but also to identify differences in legal models, mechanisms of law enforcement activities, procedures for obtaining electronic evidence, countering the use of cryptoassets and international cooperation. The use of this method makes it possible to move from a simple description of foreign experience to the definition of those legal instruments that can be adapted to the Ukrainian legal system.

Within the framework of this study, the comparative legal method is expedient to consider as a set of methods of scientific knowledge aimed at comparing legal norms, institutions, principles, procedures and organizational and legal mechanisms for combating illicit drug trafficking in cyberspace in Ukraine, the European Union and individual European states. Its use allows us to establish not only the formal similarity or difference of legal regulation, but also to find out the reasons for such differences, the effectiveness of the relevant legal mechanisms and the possibility of their application in Ukrainian conditions [1,2].

A feature of comparative legal analysis in the field of digital drug crime is the need to study several interconnected levels of legal regulation. The first level is made up of international legal standards, in particular the provisions of the United Nations (UN) convention against transnational organized crime, the United Nations (UN) convention against illicit traffic in narcotic drugs and psychotropic substances of 1988 and the Convention on Cybercrime [3-5]. The second level is formed by the regulatory legal acts of the European Union (EU) that regulates the fight against organized crime, drug trafficking, cybercrime, money laundering and access to electronic evidence. The third level is represented by the national legislation of the EU Member States. The fourth level covers the legislation and law enforcement practice of Ukraine.

An important direction of comparative legal analysis is the comparison of the conceptual and categorical apparatus. Different legal systems may use different concepts to denote organized crime, cybercrime, illegal online drug sales, digital evidence, cryptoassets and other phenomena. Therefore, the mechanical transfer of European Union (EU) terminology to Ukrainian legislation is inappropriate. The comparative legal method allows us to establish the functional meaning of the relevant concepts and determine which of them require regulatory consolidation in Ukraine.

The second important direction is the comparison of criminal legal mechanisms for combating digital drug trafficking. In this context, it is analyzed how Ukraine and European Union (EU) states define as criminally punishable the production, acquisition, storage, transportation and sale of narcotic drugs, the organization of criminal activity, participation in criminal organizations, money laundering and the use of digital technologies to implement criminal intent. At the same time, the subject of comparison is not only sanctions, but also the grounds for criminal liability, the qualification of organized criminal activity, the rules of liability of accomplices and the possibility of applying special measures to criminal assets [1,6].

Of particular importance is the comparison of legal mechanisms for combating darknet marketplaces and online platforms through which illegal drug sales are carried out. European experience demonstrates that combating such platforms is not limited to blocking a web resource. It involves conducting complex operations aimed at identifying administrators, sellers, financial operators and other network participants, seizing digital assets, analyzing electronic communications and coordinating criminal proceedings between different states [2, 7].

The comparative legal method has also been used to study the mechanisms for obtaining and using electronic evidence. This area is one of the most complex in cases of digital drug trafficking. Electronic information may be stored on servers located outside the state, belong to a foreign digital service provider, or be accessible only for a limited time. Therefore, national procedures for temporary access to electronic data, their preservation, extraction, copying, transfer, and use in criminal proceedings are compared.

Of particular importance in this regard is the European approach to European Production Orders and European Preservation Orders, aimed at increasing the efficiency of cross-border access to electronic evidence in criminal proceedings [8]. For Ukraine, this experience is important in connection with the need to improve the mechanisms for obtaining digital evidence from foreign providers and ensuring its relevance, admissibility, and reliability in criminal proceedings.

## Results and Discussion

Organized crime in the field of illicit drug trafficking in cyberspace is expediently defined as a coordinated, sustained and structured criminal activity of two or more persons aimed at organizing the production, acquisition, storage, transportation, shipment or sale of drugs using information and communication technologies.

The specificity of such crime is that cyberspace is not only an environment for the dissemination of information, but also a full-fledged element of the criminal mechanism. Digital technologies can be used to advertise drugs, search for buyers, coordinate the activities of members of an organized group, distribute roles, receive payments and hide income [9,10].

The main features of digital organized drug crime are: The use of information and communication technologies at all or most stages of criminal activity; the transnational nature of organized criminal networks; the use of anonymizing and cryptographic technologies; the use of cryptoassets or other digital financial instruments; the remote nature of interaction between the seller and the buyer; the difficulty of identifying organizers and administrators of digital platforms; rapid adaptation of criminal structures to law enforcement measures [11].

Thus, the digitalization of drug crime leads to the formation of the so-called distributed model of organized crime, in which individual participants may not contact each other directly and may not even know the true identity of the organizer of the criminal network.

The European Union (EU) is forming a multi-level system for combating illicit drug trafficking, which combines strategic planning, the activities of specialized agencies, criminal law cooperation and cybersecurity mechanisms [12].

An important place is occupied by the activities of EUDA, which monitors drug market development trends, analyzes new psychoactive substances and assesses threats associated with the digitalization of illicit drug trafficking [13].

Europol ensures coordination of the activities of law enforcement agencies of the European Union Member States (EUMS), promotes the exchange of operational information and participates in joint operations against transnational criminal networks. Of particular importance is the work of the European Cybercrime centre (EC3), which aims to combat cybercrime and support investigations into the use of digital technologies by organised crime groups [14].

Eurojust plays an important role in coordinating criminal proceedings with a cross-border dimension. In cases involving drug trafficking via digital platforms, the need to quickly obtain electronic evidence from different countries is of fundamental importance [15].

**Table 1:** European mechanisms for combating digital organized drug crime and the possibilities of their use in Ukraine.

| European mechanism | Legal and institutional framework | Practical significance | Prospects for Ukraine |
|---|---|---|---|
| Drug market monitoring | EUDA | Identifying new trends and digital sales models | Creating an integrated system for monitoring the online drug market |
| Operational information exchange | Europol | Coordinating cross-border investigations | Expanding operational cooperation between Ukrainian authorities and Europol |
| Countering cybercrime | European Center for Combating Cybercrime | Technical and analytical support to investigations | Strengthening specialized cyber units |
| Forensic coordination | Eurojust | Joint investigation teams and coordination of proceedings | More active use of international legal assistance mechanisms |
| Identifying financial flows | Anti-Money Laundering (AML)/ Countering the Financing of Terrorism (CFT) mechanisms | Tracing criminal proceeds and crypto assets | Developing control over digital financial transactions |
| Working with electronic evidence | EU mechanisms on electronic evidence | Operational acquisition of digital information | Harmonizing procedures for working with electronic evidence |

Ukraine is already facing the transformation of illicit drug trafficking into a digital environment. One of the characteristic models is the functioning of online stores, in which communication between the seller and the buyer is carried out through messengers or specialized digital platforms.

The problem is that traditional mechanisms for documenting criminal activity are often focused on physical contact between participants in illicit trafficking. In the digital model, the person administering the platform, the operator of financial transactions, the supplier of narcotics and the direct perpetrator may be located in different regions or countries.

Additional problems are the use of crypto-assets, anonymous digital wallets, Virtual Private Network (VPN) technologies, encrypted messengers and server infrastructure located outside Ukraine. This complicates the identification of the offender, determination of jurisdiction, obtaining evidence and ensuring the confiscation of proceeds from crime [16].

The legal mechanism for countering this must provide for the possibility of a comprehensive response to all elements of the digital infrastructure of the drug business. This is not only about bringing to criminal responsibility the person who directly sold drugs, but also about identifying the organizers, administrators of digital platforms, financial intermediaries and other participants in the criminal network.

Taking into account European experience, it is advisable to form a comprehensive mechanism for combating organized drug crime in cyberspace. Firstly, it is necessary to develop regulatory regulation of work with electronic evidence. Digital information should be considered not as an auxiliary, but as one of the key types of evidentiary information in criminal proceedings regarding the illegal circulation of drugs [17].

Secondly, the mechanism for identifying, arresting and confiscating crypto-assets used to finance the illegal circulation of drugs or legalizing criminal proceeds needs to be improved.

Thirdly, it is advisable to create or establish in regulations a specialized interdepartmental model for monitoring the digital drug market. Such a system can integrate the national police of Ukraine, cyber units, financial monitoring bodies, prosecutor's offices and other entities whose competence is related to combating organized crime [18].

Fourthly, it is necessary to strengthen international cooperation in the field of operational exchange of information and obtaining electronic evidence. To this end, it is advisable to make maximum use of the opportunities for cooperation with Europol, Eurojust and other international law enforcement structures [19].

Fifthly, a promising direction is the introduction of a risk-based model of analysis of digital drug crime, which will allow identifying not only individual crimes, but also connections between digital platforms, financial transactions, crypto wallets and participants in organized criminal networks.

## Conclusion

The conducted research provides grounds for formulating the following conclusions. Firstly, illicit drug trafficking in cyberspace is one of the most dynamic forms of transformation of modern organized crime. Digital technologies provide criminal networks with the opportunity to operate remotely, transnationally and with a high level of anonymity.

Secondly, cyberspace must be considered not only as an environment for committing individual crimes, but as a component of the infrastructure of modern organized drug business. Digital technologies can provide communication, advertising, coordination, financial transactions and concealment of criminal proceeds.

Thirdly, the European countermeasure model is based on the integration of law enforcement agencies, specialized agencies, criminal justice bodies and financial monitoring structures. EUDA, Europol and Eurojust play a special role.

Fourth, for Ukraine, the priority direction should be the transition from responding to individual facts of illegal drug trafficking to the systematic destruction of the entire digital infrastructure of organized criminal networks.

Fifth, the implementation of European experience should include improving procedures for working with electronic evidence, developing mechanisms for tracking and confiscating cryptoassets, strengthening interdepartmental coordination and expanding international law enforcement cooperation.

Thus, a promising model for combating organized crime in the field of illegal drug trafficking in cyberspace should be based on the principle of a comprehensive impact on the digital criminal ecosystem. Its goal should be not only to identify and prosecute individual perpetrators, but also to identify, block and eliminate the entire system of digital, organizational and financial ties that ensure the functioning of the modern drug business.

## Acknowledgement

None.

## Conflict of Interest

Authors have no conflict of interest to declare.

## References


1. United Nations Office on Drugs and Crime (UNODC). World drug report 2025, Vienna: United Nations (UN), (2025).
2. European Union Drugs Agency (EUDA). European drug report 2025: Trends and developments, Luxembourg: Publications office of the European Union (EU), (2025).
3. United Nations Office on Drugs and Crime (UNODC). World drug report 2024, Vienna: United Nations (UN), (2024).
4. Europol. Internet Organized Crime Threat Assessment (IOCTA), The Hague: European Union Agency for Law Enforcement Cooperation, (2024).
5. Eurojust. Annual report, The Hague: European Union Agency for Criminal Justice Cooperation, (2025).
6. European Union. EU drugs strategy 2021-2025. Council of the European Union (EU), (2020).
7. European parliament and council of the European Union (EU). Regulation (EU) 2023/1543 of the European parliament and of the council of 12 July 2023 on European production orders and European preservation orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Official Journal of the European Union, (2023).
8. United Nations (UN). United Nations convention against transnational organized crime, United Nations Treaty Collection, (2000).
9. United Nations. United Nations convention against illicit traffic in narcotic drugs and psychotropic substances, United Nations Office on Drugs and Crime, (1988).
10. Criminal code of Ukraine: Law of Ukraine of 05.04.2001 No. 2341-III, (2001).
11. Criminal procedure code of Ukraine. Law of Ukraine of 13 April 2012 No. 4651-VI, Official Portal of the Verkhovna Rada of Ukraine, (2012).
12. Law of Ukraine “On narcotic drugs, psychotropic substances and precursors” of 15 February 1995 No. 60/95-VR, Official Portal of the Verkhovna Rada of Ukraine, (1995).
13. Law of Ukraine “On the basic principles of ensuring cybersecurity of Ukraine” of 5 October 2017 No. 2163-VIII, Official Portal of the Verkhovna Rada of Ukraine, (2017).
14. Law of Ukraine “On prevention and counteraction to legalization (Laundering) of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction” of 6 December 2019 No. 361-IX, Official portal of the Verkhovna Rada of Ukraine, (2019).
15. V. Davydenko, M. Korniienko, A. Radchuk, A. Babiak, Y. Leheza. International cooperation in operational and search activities: A comparative analysis of foreign experience, Cadernos de Dereito Actual, 28(2025):83-102.
16. M. Korniienko, A. Desyatnik, G. Didkivska, Y. Leheza, O. Titarenko. Peculiarities of investigating criminal offenses related to illegal turnover of narcotic drugs, psychotropic substances, their analogues or precursors: Criminal law aspect, Khazanah Hukum, 5(2023):205-215.
17. O. Shkuta, Y. Leheza, I. Telelym, A. Anosienkov, O. Yaroshak. National security in the conditions of the Russia-Ukraine war: Legal regulation and Islamic law perspectives, Al-Ahkam, 34(2024):99-120.
18. O. Volobuieva, Y. Leheza, V. Pervii, Y. Plokhuta, R. Pichko. Criminal and administrative legal characteristics of offenses in the field of countering drug trafficking: Insights from Ukraine, Yustisia, 12(2023):262-277.
19. T. Voloshanivska, P. Inna, L. Serhii, M. Olha, L. Yevhen. Administrative and criminal law aspects of preventing offenses committed by minors in the sphere of illegal circulation of narcotic drugs, psychotropic substances and precursors, J Drug Alcoh Res. 12(2023).