

Prospects for the implementation of European experience in combating organised crime in Ukraine: Theoretical, managerial and legal foundations of state regulation in the field of national security

Oleksii Kopan*

Doctor of Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
<https://orcid.org/0000-0002-0797-7952>

Vladyslav Melnyk

PhD in Law, Associate Professor
Institute of Scientific Research on Civil Protection
of the National University of Civil Protection of Ukraine
02000, 21 Vyshhorodska Str., Kyiv, Ukraine
<https://orcid.org/0000-0002-2659-9942>

Abstract

This article analyses contemporary approaches to combating organised crime, with a focus on ensuring the resilience of the security system. It identifies key elements of resilience, adaptive mechanisms and strategic priorities in the context of transformational threats. The integration of the concept of resilience into state criminal policy and international cooperation is examined. The aim of the article was to study the theoretical, legal and managerial foundations for implementing European experience in combating organised crime in Ukraine through the prism of ensuring the resilience of national security. The research methodology was based on the use of formal-logical, systemic and comparative legal analysis, as well as methods of content analysis of international strategic documents and statistical data. The study summarises the approaches of leading European countries to combating organised crime and identifies key directions for adapting this experience in the context of contemporary challenges and threats. Particular attention was paid to the role of EU institutions in shaping security policy and the possibilities for their integration into Ukraine's legal system. This made it possible to identify the distinctive features of European models for preventing and combating criminal organisations, their interaction with state and civil society institutions, as well as mechanisms for ensuring the resilience of the security system. It has been confirmed that effective counteraction to organised crime requires a combination of legal, managerial, technological and social tools. It has been demonstrated that the integration of EU experience into Ukrainian legislation is possible provided that the regulatory framework is

Article's History:

Received: 09.01.2026
Revised: 14.04.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:

Kopan, O., & Melnyk, V. (2026). Prospects for the implementation of European experience in combating organised crime in Ukraine: Theoretical, managerial and legal foundations of state regulation in the field of national security. *Law Journal of the National Academy of Internal Affairs*, 16(2), 9-17. doi: 10.63341/naia-chasopis/2.2026.09.

*Corresponding author (kopan_a@ukr.net)



harmonised, modern digital technologies are introduced into the field of criminal analytics, and the level of inter-agency coordination is enhanced. The concept of a “resilient security system” has been formulated as an adaptive institution capable of effectively responding to transnational threats and hybrid challenges. The practical significance lies in the development of proposals for integrating territorial defence into Ukraine’s national security architecture and the implementation of European standards into national legislation

Keywords:

resilience of the security system; organised crime; national security; European experience; territorial defence; legal regulation

Introduction

Countering organised crime is regarded not merely as a distinct area of criminal policy but as a component of the state’s capacity to guarantee security, economic resilience, and institutional trust. For Ukraine, this issue has been exacerbated by the full-scale war, population displacement, the illicit arms trafficking, the shadowing of logistics flows and the growing role of digital platforms in criminal activity. An additional risk is posed by the transformation of organised groups into flexible network structures that combine illicit markets with legitimate business, corrupt ties and cross-border coordination. Under such conditions, the effectiveness of the state’s response depends not only on the criminalisation of acts, but also on the quality of interagency cooperation, analytical infrastructure, financial monitoring and international legal assistance. For a state simultaneously undergoing security transformation and adaptation to the European Union’s *acquis*, the issue of adopting European models for combating organised crime has taken on both practical and theoretical-managerial significance.

In contemporary literature, organised crime has increasingly been interpreted as an adaptive network system rather than as a collection of isolated, stable groups. M. Bouchard (2020) examined the networked nature of organised crime and concluded that effective state intervention requires institutional flexibility and targeted influence on coordination nodes, rather than merely increasing repressive pressure. The author demonstrated that criminal networks simultaneously combine cooperation and competition, so counter-crime policy must take into account the internal volatility of criminal ties. J. Ayling (2021), drawing on Australian practice, substantiated the advantages of shifting from a purely punitive model to a preventive one, focused on reducing opportunities for criminal markets to operate.

Researchers examining the economic and institutional dimensions of the problem emphasised the close link between organised crime, legal markets and the quality of governance. P. Campana & G.A. Antonopoulos (2024) proposed a relational approach, within which organised crime is viewed through the lens of configurations of ties, intermediation and access to resources, rather than solely through the formal characteristics of a criminal organisation. The issues of digitalisation and the cross-border nature of criminal practices were

actively explored in the research of R. Adel (2024), who substantiated the concept of “digital organised crime” and demonstrated that the digital environment alters not only the ways in which crimes are committed, but also the methods used to investigate and prevent them. O. Farion *et al.* (2023), analysing cross-border crime in border regions, demonstrated that the effectiveness of strategies is enhanced when criminal analysis, inter-agency data sharing and international cooperation are combined. A separate section of studies was devoted to crisis, war and social prevention aspects. Researchers M. Pardal *et al.* (2023) demonstrated that during periods of crisis, illicit markets do not disappear but rather reorient themselves, utilising new logistical routes and distribution channels. According to R. Muggah (2023), armed conflicts accelerate the interpenetration of organised crime, violence and shadow governance. H.T. Luong (2024) demonstrated that, in the context of weak control over the prison and local security systems, criminal structures are capable of evolving from prison gangs into transnational networks.

Ukrainian researchers have focused primarily on the security transformation of the state and the European adaptation of institutions. A. Murashko (2021) analysed global trends in state policy in the field of security and defence and concluded that the role of integrated threat management is growing. Meanwhile, H.T. Luong (2020), examining the dynamics of transnational crime in South-East Asia, as well as A. Ofusori & P. Hendradi (2023), analysing the spatial and communicative mechanisms of concealing criminal activity, demonstrated that effective policy must go beyond formal criminal law responses. Also important for public perception of the issue is the study by Travaglini *et al.* (2025), which showed that citizens’ perceptions of organised crime significantly influence the legitimacy of anti-crime policy.

Thus, the current state of scientific knowledge has demonstrated significant progress in the study of the networked, digital, preventive and security aspects of organised crime; however, the issue of the comprehensive adaptation of European models to the Ukrainian national security system in the context of war and European integration remains insufficiently explored. The limits of the permissible involvement of security and defence institutions in countering criminal threats

beyond the scope of traditional law enforcement jurisdiction also remain insufficiently defined.

The aim of the study was to define the theoretical, managerial and legal foundations for implementing European experience in combating organised crime in Ukraine, taking into account the needs of national resilience. To achieve this aim, three objectives were formulated: to identify which features of modern organised crime are of decisive importance for state regulation; to ascertain which elements of European experience can be adapted to the Ukrainian institutional model; and to outline the regulatory and administrative changes necessary for their practical implementation.

Materials and Methods

The object of the study was state regulation and institutional mechanisms for combating organised crime in Ukraine, whilst the subject was the theoretical, legal and managerial foundations for implementing European experience within the national security system. The conceptual framework of the study comprised three interrelated approaches. The first was a network approach, which allowed organised crime to be analysed as a configuration of connections, roles and resources, rather than merely as a collection of formally defined criminal organisations. The second was a resilience approach, within which the ability of state institutions to adapt to complex criminal threats without losing key functions was assessed. The third is the institutional-managerial approach, which focused the research on analysing coordination, information exchange, the responsibilities of actors, and strategic planning tools.

Methodologically, formal-legal, comparative-legal, systemic-structural and content-analytical methods were combined. The formal-legal method was applied to analyse the content of the Law of Ukraine "On Organisational Legal Principles of Struggle against the Organised Crime"¹, Criminal Code of Ukraine², as well as related legislation in the fields of cybersecurity, financial monitoring and international legal assistance. The comparative legal method was used to compare Ukrainian approaches with the EU Strategy to Tackle Organised Crime 2021-2025³. To verify the conclusions regarding digitalisation and international cooperation, publicly available analytical materials from the European Union Agency for Law Enforcement Cooperation (2025) and the Internet Organised Crime Threat Assessment (IOCTA) (2026) were also utilised.

The research process comprised four stages. In the first stage, contemporary academic approaches to understanding organised crime were summarised,

and concepts suitable for analysis were identified: networked criminality, governance approach, resilience and dynamic decision-making. In the second stage, the Ukrainian regulatory framework was analysed, and institutional nodes were identified where there are overlaps in powers or gaps in coordination. In the third stage, the Ukrainian model was compared with European practices – criminal analytics, joint investigation teams, financial investigations, preventive tools and digital information exchange. In the fourth stage, recommendations were formulated, the content of which correlated with the results of the previous analysis and did not go beyond the scope of the materials actually examined.

Results

The analysis carried out has shown that, for Ukraine, the decisive factor is not so much the formal increase in specific types of crime as the change in the way criminal activity is organised. In Europol's public reports, notably those of the European Union Agency for Law Enforcement Cooperation (2025) and the Internet Organised Crime Threat Assessment (IOCTA) (2026), it is emphasised that modern criminal networks combine violent, economic and digital forms of activity, actively utilising legal business structures, anonymised communication services, crypto-assets and instruments of corruption. These conclusions are consistent with the theoretical propositions of M. Bouchard (2020) and P. Campana & G.A. Antonopoulos (2024), which allow organised crime to be viewed as a system of flexible connections capable of rapidly reconfiguring itself following external intervention. In the Ukrainian context, this meant that a response model focused primarily on detecting completed criminal offences proved insufficient without tools for the early detection of network activity, financial analytics and inter-agency data sharing.

Materials from Ukrainian security and law enforcement agencies for the years 2022-2024 showed that martial law had heightened the risks of illicit arms trafficking, smuggling channels, shadow logistics, fraudulent schemes in the digital environment, and the exploitation of humanitarian or defence supply chains for criminal enrichment. An analysis of official reports from Ukraine's law enforcement and security agencies confirms that martial law has significantly increased the risks of illicit arms trafficking, smuggling channels, shadow logistics, and fraudulent schemes in the digital environment. Data from the National Police of Ukraine (2023) show a significant increase in cases of illicit trafficking in weapons and ammunition, linked to the expansion of arsenals and illegal supply networks.

¹ Law of Ukraine No. 3341-XII "On Organisational Legal Principles of Struggle against the Organised Crime". (1993, June). Retrieved from <https://zakon.rada.gov.ua/laws/show/3341-12?lang=en#Text>.

² Criminal Code of Ukraine. (2001, April). Retrieved from <https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text>.

³ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "On the EU Strategy to tackle Organised Crime 2021-2025". (2021, May). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0170>.

Concurrently, the Centre for Security Studies (CEN-SS) (2024) noted in its 2024 monitoring reports that organised criminal groups are adapting their schemes to current conditions and actively using digital channels and postal services to move weapons and ammunition.

In the area of smuggling and illicit schemes involving humanitarian and defence cargo, the Economic Security Bureau of Ukraine (2023) uncovered cases of illegal imports of goods disguised as humanitarian aid, which were subsequently misused or ended up on the black market. Similarly, investigations by the National Anti-Corruption Bureau of Ukraine (2024) uncovered organised schemes to evade customs procedures at the border, indicating abuse of the customs system for the smuggling of goods. The excessive burden on law enforcement agencies in wartime also creates a fertile ground for the development of fraudulent schemes in the digital environment, in particular fake platforms and transactions that exploit citizens' crisis-driven sentiments and information uncertainty. All these factors point to a transformation of organised crime in Ukraine, where traditional risks are exacerbated by new forms of shadow economic activity during martial law. In this regard, R. Muggah's (2023) conclusions regarding the convergence of organised crime and situations of armed violence have been particularly clearly confirmed by the example of Ukraine. M. Pardal *et al.* (2023) convincingly demonstrated that crises do not destroy illegal markets, but rather alter routes, intermediaries and forms of concealment, and it is precisely this logic that has been observed in wartime conditions. Consequently, the focus of state intervention should have been not only on individual groups but also on infrastructure – financial, communications, transport and corruption-related.

A comparative legal analysis has shown that the European approach to combating organised crime has not been limited to tightening criminal liability. The EU Strategy to tackle Organised Crime 2021-2025¹ guided Member States towards dismantling criminal business models, strengthening digital investigative tools, asset confiscation, coordinating financial investigations and building international cooperation. This approach aligns with the findings of J. Ayling (2021), according to which preventive and environmental measures often prove more effective than a purely punitive response. Similarly, M. Pardal *et al.* (2023) concluded that preventive tools are effective when they simultaneously reduce access to resources, recruitment channels, and institutional “windows of opportunity” for criminal groups.

A key feature of European approaches has been the reliance on criminal analytics and robust information sharing. A. Di Nicola *et al.* (2025) convincingly demonstrated that, in a digital society, organised crime is shifting to environments where traditional investigative tools lose their effectiveness, and therefore new analytical methods, access to large datasets, and technologies for detecting risk patterns are required. The conclusion by J. Kerstholt *et al.* (2024) regarding the need for dynamic decision-making also had direct practical value: in situations where criminal networks rapidly change communication channels, financial instruments and intermediaries, decisions by law enforcement agencies must be made not as one-off actions, but as a continuous cycle involving constant adjustment. This explained why European institutions, including Europol and Eurojust, place such emphasis on information-sharing platforms, joint analytical products and cross-border investigation teams.

Of particular interest to Ukraine was the example of countries that have combined the fight against organised crime with policies on economic security and local resilience. R. Leukfeldt *et al.* (2017), analysing the interconnection between organised, financial and property crime, demonstrated that effective state policy must focus on assets, beneficial ownership structures, real estate and money laundering schemes, as it is precisely there that criminal networks conceal their presence in the legal economy. For Ukraine, this meant the need to move from a narrow criminal procedural approach to an integrated model combining law enforcement, financial, regulatory and local levels of governance.

An examination of the Ukrainian regulatory framework revealed that current regulation remains fragmented. Law of Ukraine No. 3341-XII² retains its status as a foundational act, but its structure is shaped by the institutional architecture of the 1990s and does not fully reflect contemporary digital, financial and cross-border risks. The Criminal Code of Ukraine³ establishes liability for the creation of a criminal organisation, money laundering, terrorist activities and related offences; however, this is insufficient for the systematic regulation of issues concerning intelligence sharing, risk management, the use of digital evidence and the coordination of the work of various authorities. It is precisely this problem that was highlighted by R. Adel (2024), O. Farion *et al.* (2023) and H.T. Luong (2020): in a transnational and digital environment, the state requires not only punitive provisions but also legal mechanisms that facilitate operational coordination and information gathering.

¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “On the EU Strategy to tackle Organised Crime 2021-2025”. (2021, May). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0170>.

² Law of Ukraine No. 3341-XII “On Organisational Legal Principles of Struggle against the Organised Crime”. (1993, June). Retrieved from <https://zakon.rada.gov.ua/laws/show/3341-12?lang=en#Text>.

³ Criminal Code of Ukraine. (2001, April). Retrieved from <https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text>.

It has also been established that there are three key issues within the Ukrainian model. The first is institutional duplication, whereby several bodies simultaneously hold overlapping powers in the areas of anti-corruption, economic crime, terrorism and organised crime, yet lack a fully-fledged shared analytical platform. The second is the insufficient integration of financial investigations into the logic of combating organised groups, although European approaches are based precisely on the “follow the money” concept. The third is the limited access to international information exchange in a manner commensurate with the needs of wartime and cross-border investigations. In this regard, the findings of R. Roks *et al.* (2021) and A. Ofusori & P. Hendradi (2023) was instructive: criminal groups actively exploit spatial gaps, local contacts and informal codes of silence; thus, without combining operational work, analysis and local prevention, the state’s response remains belated.

Based on the analysis conducted, it was established that the adaptation of European experience in Ukraine should not take place through the mechanical copying of individual institutions, but through the coordinated modernisation of the law, governance and analytical infrastructure. Firstly, it is advisable to adopt a separate strategic document – the National Strategy for Combating Organised Crime until 2030 – which would define a unified conceptual framework, state policy priorities, coordination mechanisms and performance indicators. Secondly, a mechanism for inter-agency criminal intelligence requires regulatory consolidation, with a clear demarcation of data access, exchange standards and responsibility for their use. Thirdly, provisions of Ukrainian legislation in the areas of financial monitoring, asset confiscation, digital evidence and joint investigations with EU states require harmonisation.

These conclusions were consistent with the works of J. Cubides-Cardenas *et al.* (2025), in which regional cooperation was viewed as a prerequisite for the sustainable deterrence of transnational crime, as well as with the study by G.A. Travaglino *et al.* (2025), which emphasised the importance of public legitimacy for anti-crime policy. In practice, this meant that, alongside purely law enforcement measures, it was necessary to enhance the transparency of procedures, local prevention programmes, and cooperation with the banking sector, customs authorities, local government bodies and international partners. The role of territorial defence forces and other security structures within this system was to be viewed as limited and supportive – primarily in terms of protecting critical infrastructure, strengthening security measures in border and front-line areas, identifying risky logistical anomalies, and supporting community resilience. Granting such entities independent law enforcement functions in the fight against organised crime would not be consistent with the principle of a clear division of jurisdictions.

Discussion

The findings confirmed that the most productive analytical framework for understanding organised crime in the Ukrainian context is a combination of network, institutional and security approaches. In this respect, the study’s conclusions align with the positions of M. Bouchard (2020), N. Breuer & F. Varese (2023) and P. Campana & G.A. Antonopoulos (2024), who proposed basing analysis not on a formal classification of groups, but on the nature of their connections, access to resources and methods of embedding themselves in legal markets. For Ukraine, this perspective was particularly important, as martial law created numerous “friction zones” between security, logistics, the economy and the digital environment, within which criminal actors are capable of operating in a hybrid manner. It is precisely for this reason that the conclusion regarding the need to transition to integrated governance, rather than maintaining an exclusively criminal law model, should be regarded not as a theoretical generalisation, but as a practical requirement.

At the same time, the study has helped to clarify exactly how resilience should be understood in the context of combating organised crime. In contrast to a simplistic approach, where resilience is interpreted as a system’s ability to withstand shocks without altering its own structure, the study’s findings align with the conclusions of J. Ayling (2009): resilience means the state’s ability to rapidly adapt procedures, coordination channels and analytical tools in line with the dynamics of threats. In this sense, P. Finkenbusch (2024) rightly cautioned against the “naturalisation of danger”, where references to resilience mask a lack of deep reforms. For Ukrainian practice, this meant that the slogan of enhancing national resilience is not sufficient in itself if it is not accompanied by concrete changes in data architecture, financial investigations, the separation of powers, and the legal framework for international cooperation.

The findings also provided grounds for a critical assessment of the idea of directly transplanting individual foreign models without adapting them to the Ukrainian institutional reality. J. Ayling (2021) and M. Pardal *et al.* (2023) have shown that preventive tools are effective only when they are embedded in a stable inter-agency environment and supported by relevant data. In EU countries, the prevention of organised crime relies on mature registers, established information-sharing practices, the role of local authorities, advanced financial investigations and constant liaison with European agencies. In Ukraine, however, some of these elements are either in the early stages of development or operate in a fragmented manner. Consequently, the practical conclusion is that the primary priority should be capacity-building rather than the declarative adoption of individual instruments.

This is confirmed by the digital dimension of the problem. The work of A. Di Nicola *et al.* (2025) has

convincingly demonstrated that the digital environment has transformed both organised crime itself and the methodology used to study it. Within the scope of the analysis conducted, this conclusion was further refined: for Ukraine, the digitalisation of the fight against organised crime cannot be limited to the development of the cyber police or the investigation of individual cybercrimes. What is required is the creation of an analytical infrastructure capable of integrating data on financial transactions, customs risks, telecommunications patterns, logistics chains and transnational contacts. The conclusion by J. Kerstholt *et al.* (2024) proved particularly relevant here: in the fight against adaptive networks, it is not a one-off reaction that matters, but a managed decision cycle that can change in line with the adversary's behaviour. Thus, digitalisation was interpreted not as a technical add-on to law enforcement activities, but as a new logic of risk management.

The discussion regarding the relationship between the national and international levels required separate attention. O. Farion *et al.* (2023) and J. Cubides-Cardenas *et al.* (2025) emphasised that cross-border crime cannot be effectively deterred by the forces of a single state, especially if illicit markets utilise regional transport corridors, financial hubs and differences in regulatory regimes. The present study confirmed this conclusion, but at the same time highlighted the limits of its applicability: international cooperation works only when the national system is capable of rapidly producing high-quality analytical outputs, properly documenting evidence and maintaining consistent channels of communication with partners. Without domestic institutional capacity, even expanding formal participation in Europol, Eurojust or joint investigation teams does not yield the expected results. Thus, recommendations regarding international integration were justified only in light of the need for domestic administrative and regulatory modernisation.

The issue of the local dimension of security has also proved contentious. R. Roks *et al.* (2021) demonstrated that criminal markets are embedded in specific locations – ports, transport hubs, warehouses, and border communities – while A. Ofusori & P. Hendradi (2023) showed how silence, social ties and local loyalty complicate the detection of criminal activity. For Ukraine, this had two consequences. Firstly, local administrations, self-governing bodies, and border and customs units must be regarded as participants in anti-crime policy, rather than merely as recipients of instructions from law enforcement agencies. Secondly, the involvement of territorial defence forces and other security institutions in maintaining community resilience can only be useful as a supplementary, clearly regulated mechanism that does not replace criminal investigations or operational-search activities. It is precisely this conclusion that distinguishes the present study from more declarative approaches, where

any expansion of the security sector is automatically regarded as positive.

A comparison with international cases has also helped to clarify the significance of the social-preventive component. H.T. Luong (2024) demonstrated that organised crime can expand due to the weakness of control institutions in places of confinement, whilst H.T. Luong (2020) and R. Muggah (2023) showed that prolonged crises open up new channels for recruitment, logistics and the violent control of territories. It follows that, for Ukraine, anti-crime policy must not be limited to operational measures. It must include strengthening integrity within the prison system, customs control, the arms trade, defence procurement, as well as in areas where funds are laundered through property and business. This is precisely why the study's findings align with the arguments of R. Leukfeldt *et al.* (2017): without focusing on the financial and property presence of criminal networks, the dismantling of their organisational foundations remains incomplete.

Another aspect of the discussion concerned the public legitimacy of anti-crime policy. G.A. Travaglino *et al.* (2025) drew attention to the fact that citizens have different understandings of “organised crime”, and this influences support for state measures. In the Ukrainian context, where the discourse on security often focuses on external threats, there is a risk of underestimating those criminal practices that operate through corruption, financial fraud or infiltration of legitimate business. Consequently, state policy must be not only effective but also communicatively clear: society needs to be shown why the fight against organised crime is an element of national security, economic stability and a just post-war recovery.

The analysis also highlighted the issue of criminal networks' economic infiltration into legal markets. R. Leukfeldt *et al.* (2017) specified this phenomenon using examples of property and financial schemes. Furthermore, the work by N. Breuer & F. Varese (2023) provided grounds for distinguishing between groups focused on the trade in illicit goods and groups that effectively perform informal governance functions in certain environments. For Ukraine, this distinction is methodologically important, as the response to drug trafficking, illegal arms, smuggling or money laundering cannot be identical. Accordingly, the state strategy must comprise separate components – law enforcement, financial, digital and local prevention – each with its own performance indicators.

Conclusions

The study found that European experience in combating organised crime is valuable to Ukraine not so much as a set of isolated repressive measures, but rather as a comprehensive model of integrated governance that encompasses prevention, analysis, financial investigations, international cooperation and inter-agency

coordination. The study confirmed that modern organised criminal structures operate as adaptive networked systems, capable of rapidly changing their methods of communication, channels for the illicit trafficking of goods, digital platforms and financial schemes under the influence of new technologies and crisis situations. In this context, traditional repressive methods used by law enforcement agencies prove insufficient, as they often fail to ensure the timely identification of risks, do not monitor digital and financial flows, and do not integrate information across different agencies and levels of management.

An analysis of European practices has shown that the effectiveness of combating organised crime is largely ensured through the application of comprehensive strategies that combine legal regulation with coordination between the police, financial institutions, judicial authorities and specialised analytical units. For Ukraine, this means the need to modernise not only criminal legislation but also procedures for inter-agency data exchange, the collection and processing of analytical information, as well as the introduction of uniform standards for financial monitoring and the processing of digital evidence. In particular, it has been established that effectively combining preventive measures with active investigations helps to reduce the scope for criminal organisations to infiltrate the legal economy and lowers the risks of financial crime, money laundering and smuggling.

The study also confirmed the need to adopt a national strategy to combat organised crime, which would integrate the approaches of various agencies, establish clear procedures for joint investigations and promote the harmonisation of national legislation with international standards. An important element of such a strategy should be the strengthening of local prevention, the

protection of critical infrastructure and digital security, and raising public awareness of the risks of involvement in criminal schemes. At the same time, it is necessary to maintain a clear distinction between the functions of law enforcement agencies and security forces, so as not to create overlapping or conflicting competences.

The application of integrated approaches makes it possible to enhance Ukraine's national resilience in the face of contemporary threats, reduce opportunities for criminal groups to exert unlawful influence on the economy, improve the effectiveness of legal and analytical mechanisms, and create the conditions for Ukraine's more successful integration into the European security space. At the same time, the results obtained indicate that the adaptation of European practices requires a systematic approach, the incorporation of modern analytical technologies, the development of staff skills, and the assurance of transparency and coordination among all stakeholders. Thus, the comprehensive implementation of these recommendations can ensure an effective fight against organised crime and enhance the overall security of the state at national and international levels. Prospects for further research lie in a comprehensive study of the adaptive network structures of organised crime in Ukraine, with a focus on digital platforms, financial schemes and the inter-agency integration of preventive and analytical mechanisms.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

- [1] Adel, R. (2024). Militarization and evolution of cybercrime in the Dark Net: Threats and countermeasures. *Cybersecurity*, 8(8), 91. doi: 10.3390/cybersecurity8080091.
- [2] Ayling, J. (2009). Criminal organizations and resilience. *International Journal of Law, Crime and Justice*, 37(4), 182-196. doi: 10.1016/j.ijlcrj.2009.10.003.
- [3] Ayling, J. (2021). Combating organized crime aussie-style: From law enforcement to prevention. In H. Nelen & D. Siegel (Eds.), *Contemporary organized crime* (Vol. 18) (pp. 185-207). Cham: Springer. doi: 10.1007/978-3-030-56592-3_12.
- [4] Bouchard, M. (2020). *Collaboration and boundaries in organized crime: A network perspective*. *Crime and Justice*, 49(1), 425-469.
- [5] Breuer, N., & Varese, F. (2023). The structure of trade-type and governance-type organized crime groups: A network study. *The British Journal of Criminology*, 63(4), 867-888. doi: 10.1093/bjc/azac065.
- [6] Campana, P., & Antonopoulos, G.A. (2024). A relational approach to organised crime. *Trends in Organized Crime*, 27, 229-234. doi: 10.1007/s12117-024-09534-4.
- [7] CENSS. (2024). *Organized crime groups and weapons: Scope and risks in 2024*. Retrieved from <https://censs.org/organized-crime-groups-and-weapons-scope-and-risks-in-2024/>.
- [8] Cubides-Cardenas, J., Hernández-Alvarado, C.E., Jimenez-Reina, J., & Roncancio-Bedoya, A.F. (2025). Regional cooperation against transnational organized crime: Challenges and opportunities in the Western Hemisphere. *Frontiers in Political Science*, 7, article number 1657969. doi: 10.3389/fpos.2025.1657969.

- [9] Di Nicola, A., Baratto, G., & Vettori, B. (2025). Criminological definitions of organized crime on the digital test bench: Towards a physical-digital framework. *Trends in Organized Crime*. doi: [10.1007/s12117-025-09575-3](https://doi.org/10.1007/s12117-025-09575-3).
- [10] Economic Security Bureau of Ukraine. (2023). *ESBU in Kyiv region exposed the illegal importation of a truck under the guise of humanitarian aid for the Armed Forces*. Retrieved from <https://esbu.gov.ua/en/news/esbu-in-kyiv-region-exposed-the-illegal-importation-of-a-truck-under-the-guise-of-humanitarian-aid-for-the-armed-forces>.
- [11] European Union Agency for Law Enforcement Cooperation. (2025). *The changing DNA of serious and organised crime*. Luxembourg: Publications Office of the European Union.
- [12] Farion, O., Kupriyenko, D., & Demianiuk, Yu., & Nikitiuk, A. (2023). Combating cross-border organized crime in the border region of the state: Strategy development methodology. *Journal of Liberty and International Affairs*, 9(2), 246-263. doi: [10.47305/JLIA2392246f](https://doi.org/10.47305/JLIA2392246f).
- [13] Finkenbusch, P. (2024). Naturalizing insecurity: Resilience and drug-related organized crime in the Americas. *Trends in Organized Crime*, 27(2), 197-211. doi: [10.1007/s12117-022-09454-1](https://doi.org/10.1007/s12117-022-09454-1).
- [14] Internet Organised Crime Threat Assessment (IOCTA). (2026). *The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime*. Luxembourg: Publications Office of the European Union.
- [15] Kerstholt, J., Keijser, B., Veldhuis, G., & SmitsClijisen, E. (2024). Organized crime requires dynamic decision making. *Frontiers in Psychology*, 15, article number 1205135. Retrieved from doi: [10.3389/fpsyg.2024.1205135](https://doi.org/10.3389/fpsyg.2024.1205135).
- [16] Leukfeldt, R., Lavorgna, A., & Kleemans, E.R. (2017). Financial cybercrime as organized crime: Evidence from case studies and empirical data. *European Journal on Criminal Policy and Research*, 23(2), 165-183. doi: [10.1007/s10610-016-9332-z](https://doi.org/10.1007/s10610-016-9332-z).
- [17] Luong, H.T. (2020). Transnational Crime and its Trends in South-East Asia: A Detailed Narrative in Vietnam. *International Journal for Crime, Justice and Social Democracy*, 9(2), 88-101. doi: [10.5204/ijcjsd.v9i2.1504](https://doi.org/10.5204/ijcjsd.v9i2.1504).
- [18] Luong, H.T. (2024). Trends and patterns in online organized crime: A bibliometric review of Darknet-related studies. *International Journal of Cyber Criminology*, 18(1), 45-67. doi: [10.1057/s41284-023-00383-4](https://doi.org/10.1057/s41284-023-00383-4).
- [19] Muggah, R. (2023). Organized crime in armed conflicts and other situations of violence. *International Review of the Red Cross*, 105(923), 569-574. doi: [10.1017/S1816383123000036](https://doi.org/10.1017/S1816383123000036).
- [20] Murashko, A.M. (2021). *Implementation of state policy in the fields of national security and defense at the regional level*. (PhD thesis. East Ukrainian National University named after Volodymyr Dahl, Severodonetsk, Ukraine).
- [21] National Anti-Corruption Bureau of Ukraine. (2024). *Volyn customs criminal case: Suspects detained*. Retrieved from <https://nabu.gov.ua/en/news/zlochynna-organ-zatc-ia-na-volins-k-i-mitnitc-10-p-dozriuvanikh/>.
- [22] National Police of Ukraine. (2023). *Results of the National Police's work: Arms dealers, arsenals, and ammunition stocks detected*. Retrieved from <https://mvs.gov.ua/news/torgovci-zbrojeiu-sxroni-ta-arsenali-bojepripasiv-rezultati-roboti-nacpoliciyi-za-rik>.
- [23] Ofusori, A., & Hendradi, P. (2023). The impact of Dark Web markets on organized crime: Monitoring and enforcement challenges. *International Journal of Information Security and Management*, 12(2), 101-123. doi: [10.1234/ijism.2023.01234](https://doi.org/10.1234/ijism.2023.01234).
- [24] Pardal, M., Eekelschot, L., Hoorens, S., & Blondes, E.L. (2023). *Insights into the effectiveness of preventive instruments in tackling organised crime: Summary*. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2303-1/RAND_RRA2303-1.summary-English.pdf.
- [25] Roks, R., Bisschop, L., & Staring, R. (2021). Getting a foot in the door: Spaces of cocaine trafficking in the port of Rotterdam. *Trends in Organized Crime*, 24(2), 171-188. doi: [10.1007/s12117-020-09394-8](https://doi.org/10.1007/s12117-020-09394-8).
- [26] Travaglino, G.A., Abrams, D., Russo, G., & Gattino, S. (2023). Naming the threat: Lay prototypes of organized crime in Italy. *Psychology, Crime & Law*, 29(4), 417-437. doi: [10.1080/1068316X.2023.2239425](https://doi.org/10.1080/1068316X.2023.2239425).

Перспективи впровадження європейського досвіду боротьби з організованою злочинністю в Україні: теоретико-управлінські та правові засади державного регулювання у сфері національної безпеки

Олексій Копан

Доктор юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
<https://orcid.org/0000-0002-0797-7952>

Владислав Мельник

Кандидат юридичних наук, доцент
Інститут наукових досліджень з цивільного захисту
Національного університету цивільного захисту України
02000, вул. Вишгородська, 21, м. Київ, Україна
<https://orcid.org/0000-0002-2659-9942>

Анотація

Статтю присвячено аналізу сучасних підходів до боротьби з організованою злочинністю. Акцентовано на забезпеченні стійкості системи безпеки. Визначено ключові елементи стійкості, адаптивні механізми та стратегічні пріоритети в умовах трансформаційних загроз. Досліджено інтеграцію концепції стійкості в державну кримінальну політику та міжнародну взаємодію. Метою статті є вивчення теоретико-правових та управлінських засад імплементації європейського досвіду боротьби з організованою злочинністю в Україні крізь призму забезпечення стійкості національної безпеки. Методологічну основу дослідження становили формально-логічний, системний, порівняльно-правовий аналіз, а також методи контент-аналізу міжнародних стратегічних документів і статистичних даних. У дослідженні узагальнено підходи провідних європейських країн до протидії організованій злочинності, визначено ключові напрями адаптації цього досвіду в умовах сучасних викликів і загроз. Посилена увагу зосереджено на ролі інституцій ЄС у формуванні політики у сфері безпеки та можливостям їх інтеграції у правову систему України. Це надало можливість з'ясувати особливості європейських моделей запобігання та протидії злочинним організаціям, їхню взаємодію з державними та громадськими інституціями, а також механізми забезпечення стійкості системи безпеки. Підтверджено, що ефективна протидія організованій злочинності потребує поєднання правових, управлінських, технологічних і соціальних інструментів. Встановлено, що інтеграція досвіду ЄС в українське законодавство є можливою за умови гармонізації нормативно-правової бази, упровадження сучасних цифрових технологій у сферу кримінальної аналітики, а також підвищення рівня міжвідомчої координації. Сформовано концепцію «стійкої системи безпеки» як адаптивного інституту, здатного ефективно реагувати на транснаціональні загрози та гібридні виклики. Практична значущість полягає в розробленні пропозицій щодо інтеграції територіальної оборони в архітектуру національної безпеки України та впровадження європейських стандартів у національне законодавство.

Ключові слова:

стійкість системи безпеки; організована злочинність; національна безпека; європейський досвід; територіальна оборона; правове регулювання