

DOI <https://doi.org/10.30525/2592-8813-2026-1-3>

AIDING THE AGGRESSOR STATE: METHODS, FORMS, AND JUDICIAL PRACTICE

Andrii Heletei,

*Lieutenant Colonel of the Security Service of Ukraine (SBU),
Master of Psychology, Postgraduate Student,
National Academy of the Security Service of Ukraine (Kyiv, Ukraine)
ORCID ID:0009-0002-3639-020X
andriy.geletey@icloud.com*

Abstract. The article examines the concepts of “aiding the aggressor state” and “collaborationism” in the context of the ongoing armed conflict in Ukraine. Various methods of committing the crime are analyzed, including military, financial, political, informational, and technical support to the aggressor, as well as the transfer of intelligence data and participation in separatist movements. The study highlights the manifestation of aiding in digital environments and through international financial and communication channels. Judicial practice and scholarly approaches to the qualification of these offenses are reviewed, emphasizing the complexity of proving intent and the importance of interdisciplinary methods, including forensic psychological examination. The article stresses the need for a comprehensive response combining legal, social, and psychological mechanisms to effectively prevent and investigate crimes that threaten national security and state stability.

Key words: aiding the aggressor state, collaborationism, Article 111-2, criminal liability, armed conflict, military assistance, financial support, political assistance, informational warfare, cyber assistance, internal intent, forensic investigation, judicial practice, prevention, prosecution.

Problem Statement. The legal regulation of collaborationist activities and aiding an aggressor state under the conditions of an armed conflict is extremely relevant today. Despite the existence of specific provisions in the Criminal Code of Ukraine (Articles 111-1 and 111-2), the lack of a clear distinction between these criminal offenses in law-enforcement practice creates legal uncertainty, which may lead to inconsistent application of criminal law. At the same time, technological development, globalization, and the expansion of digital communications have significantly broadened the range of possible forms of aiding an aggressor state, including financial, political, informational, and technical assistance. This necessitates a systematic analysis of the methods of committing this crime and the formulation of clear criteria for differentiating collaborationism from aiding an aggressor state.

State of Research. The issue of criminal liability for aiding an aggressor state is relatively new, given its actualization in connection with the realities of armed conflict and the introduction of relevant legal norms into national legislation. Scholarly literature addresses various aspects of this issue, including forms of intentional actions aimed at assisting the aggressor state, judicial practice, and problems of criminal qualification (Dopiriak; Zahyney-Zabolotenko, 2024; Dudorov; Movchan, 2022; Mishchuk, 2023). Attention is paid to issues of collaborationist activity and its differentiation from aiding the aggressor state (Mokina, 2025; Shvets, 2025), as well as to the relationship between the method of committing the crime and the personality of the offender (Orzhynska; Senina, 2022). Theoretical and legal problems of criminalizing aiding the aggressor state have been examined within the framework of modern Ukrainian criminal law (Politova; Lehunova, 2025; Shlapachenko, 2023). At the same time, the problem of proving the subjective element of the crime, particularly internal intent, remains complex and requires further scholarly reflection, especially with regard to the use of forensic and forensic-psychological research methods.

The purpose of this study is to comprehensively examine the methods of committing the crime provided for in Article 111-2 of the Criminal Code of Ukraine under contemporary conditions of armed conflict, to clearly distinguish collaborationist activity from aiding an aggressor state, and to

develop recommendations aimed at improving the effectiveness of law enforcement and strengthening national security through the integration of criminal-law and socio-psychological approaches to counteracting this category of crimes.

Main Content. In law-enforcement practice, one of the most controversial issues of contemporary Ukrainian criminal law is the differentiation between the elements of crimes provided for in Articles 111-1 (“Collaborationist Activity”) and 111-2 (“Aiding an Aggressor State”) of the Criminal Code of Ukraine. The relevance of this issue is обусловлена both by the novelty of these legal norms and by the specific conditions of the armed aggression of the Russian Federation against Ukraine, under which a significant number of socially dangerous acts have a mixed or multi-component character.

Despite their common focus on protecting Ukraine’s national security, the criminal-law purposes of these norms differ substantially, which necessitates clear doctrinal and practical differentiation.

The immediate object of the crime provided for in Article 111-1 of the Criminal Code of Ukraine is social relations in the sphere of ensuring sovereignty, territorial integrity, and the constitutional order of exercising public power in temporarily occupied territories. Collaborationist activity primarily encroaches upon the legitimacy of Ukrainian state authority by creating conditions for the functioning and consolidation of the occupation regime. Such acts are aimed at the institutionalization and stabilization of the occupier’s power through participation in occupation bodies, implementation of regulatory, administrative, or educational standards of the aggressor state, and public support of decisions made by illegal occupation administrations.

In contrast, the crime provided for in Article 111-2 of the Criminal Code of Ukraine has a different immediate object—Ukraine’s defense capability and national security in the military, economic, and informational spheres. Aiding an aggressor state consists in providing assistance that objectively enhances the aggressor’s ability to carry out armed aggression or other hostile actions against Ukraine. This includes, *inter alia*, the transfer of military-related information, logistical or material support for the armed formations of the Russian Federation, financing, technological or organizational assistance, as well as facilitating the activities of the aggressor state’s intelligence services (Dudorov; Movchan, 2022)

Thus, the key criterion for differentiating these offenses lies in the functional orientation of the act. Collaborationist activity is oriented toward establishing and maintaining control over territory and population, that is, toward ensuring the administrative capacity of the occupation authorities. Aiding an aggressor state, in turn, is aimed at achieving a specific military, economic, or informational result that strengthens the aggressor’s capabilities in confrontation with Ukraine.

Differences are also evident in the characteristics of the subject of the crime. By its nature, collaborationist activity presupposes active participation in quasi-public relations and is generally associated with the offender’s presence in temporarily occupied territory and the performance of functions related to governance or public activity. Aiding an aggressor state, however, may be committed by any natural person, regardless of citizenship, place of residence, or formal connection with the occupation administration.

In practice, situations of concurrence or aggregation of criminal norms may arise, where the same individual simultaneously participates in the activities of occupation bodies and provides direct assistance to the military or intelligence services of the Russian Federation. In such cases, qualification should be determined with regard to the factual role of the person and the dominant orientation of their actions. If the core content of the conduct consists in facilitating warfare against Ukraine, priority should be given to qualification under Article 111-2 of the Criminal Code of Ukraine, even if such actions were carried out under the guise of administrative or “civil” activity (Mishchuk, 2023).

Therefore, proper differentiation between collaborationist activity and aiding an aggressor state is of fundamental importance for ensuring uniform law enforcement and the realization of the principle of fairness in criminal liability under conditions of armed conflict.

At the same time, scholars propose various methods of committing the crime of aiding an aggressor state, «including: transferring to officers of the Russian FSB any available information about servicemen of the “Azov” regiment, participants of the ATO/JFO, pro-Ukrainian citizens, law-enforcement officers, volunteers, and others; assisting occupiers in loading grain for so-called “export”; discrediting Ukrainian state authorities; implementing and supporting decisions of occupation authorities aimed at the illegal integration and functioning of the Russian banking system in temporarily occupied territories; organizing inventories of material assets of higher education institutions, and other actions» (Orzhynska; Senina, 2022 : 102).

In our view, the listed methods do not exhaust all possible ways of committing this crime. Therefore, further analysis is required to consistently present our reasoning.

Next, we examine the forms in which aiding an aggressor state may manifest itself.

The first and most obvious form of aiding an aggressor state consists in providing it or its controlled structures with means that enable the initiation or continuation of military operations. These may include supplies of weapons, equipment, ammunition, or other military products that directly contribute to the escalation of the conflict. However, under modern conditions, aiding increasingly takes more complex and indirect forms, such as financial, logistical, or other support that ensures the functioning of the aggressor’s military machine at all stages of the war. For example, financing the modernization of military infrastructure, providing resources for the creation of new military bases, or supporting such initiatives through commercial entities constitutes assistance no less significant than the direct supply of armaments.

One of the most significant forms of aiding an aggressor state is financial assistance. This may include both direct monetary transfers and investments in enterprises that contribute to the development of the aggressor’s economy. Companies specializing in the production of military equipment and ammunition, as well as enterprises involved in the transportation, supply, or maintenance of military forces, often become the primary recipients of such investments. For example, state support of major energy companies that ensure the supply of energy resources for the military-industrial complex, or the financing of new manufacturing facilities producing military equipment, undoubtedly enhances the aggressor’s ability to continue hostilities.

Detecting such financial flows requires comprehensive investigations, particularly through identifying international financial networks that may be used to finance aggression. This includes the analysis not only of direct transactions but also of complex smuggling schemes involving intermediaries such as shell companies or fictitious organizations (Shvets, 2025)

In such cases, an essential role is played by modern technologies for big data analysis, as well as specialized methods for tracing financial flows through multiple intermediary links. Although this significantly complicates counteraction, it remains critically important for international security.

Political and diplomatic aiding occupies a central place in the context of international relations, as it may have profound consequences for global stability and security. Support provided through political and diplomatic channels is not always limited to official acts or governmental declarations. Informal mechanisms of influence are often equally important, including private contacts between high-ranking officials or influential political actors who may use their status to support the aggressor or facilitate the realization of its interests.

A key element of political aiding consists in support expressed through public statements or coordinated diplomatic actions demonstrating alliance with or understanding of the aggressor. Such actions may take the form of public endorsements at international forums that justify or legitimize aggressive behavior, or abstention from condemnation within international organizations such as the United Nations or the European Union. This may also include voting on resolutions that enable the aggressor to pursue its policies without international accountability.

Another important form of political aiding involves diplomatic agreements that may serve as a façade for supporting aggression. These may include agreements providing economic, military, or other forms of assistance to the aggressor state, as well as the creation of strategic alliances that strengthen the aggressor's position on the international stage. Such agreements may form part of covert arrangements concealed from the public and the international community.

In this context, private channels of influence are no less significant. Individuals holding high public office may, through informal meetings, personal connections, or corporate interests, implement political decisions favorable to the aggressor. These may include closed-door meetings, unofficial diplomatic channels, or direct agreements between political actors that bypass formal procedures and provide diplomatic or political support for aggression (Mokina, 2023)

The analysis of political statements, diplomatic agreements, and channels of interaction between states is crucial for identifying actors who facilitate aggressive actions. Detailed examination of such materials helps uncover hidden intentions and strategies of support for the aggressor and enables the anticipation of potential diplomatic steps that may either intensify or mitigate aggressive tendencies on the international stage.

Acts of aiding, unlike collaborationism, are not confined by geographical boundaries, which is particularly significant in the modern world where virtual communication has become pervasive. Collaborationism is traditionally associated with cooperation with an enemy or occupation authorities within occupied territories, limited to a specific state or region. However, in a globalized environment characterized by instant communication and information exchange, geographical borders no longer serve as effective barriers to acts of aiding (Politova; Lehunova, 2025).

The Internet, social networks, and other digital platforms allow individuals and organizations across the globe to establish connections that facilitate aggressive actions even when they are physically located far from the conflict zone. These may include transnational corporations providing resources, financial institutions supporting illicit transactions, or individuals cooperating online with the aggressor by transferring information, funds, or technologies that sustain aggression. In this context, even geographically distant actions may have a substantial impact on the conflict.

Virtual communication, free from physical constraints, creates new opportunities for aiding an aggressor state. Individuals may cooperate through cyberattacks, target identification, information gathering and dissemination that undermine national security, or through the exploitation of financial systems to evade sanctions or support illegitimate regimes. Data-exchange technologies enable the creation of communication channels in which participants and their actions are difficult to trace, while virtual tools may be used to spread propaganda or disinformation, contributing to conflict escalation.

Thus, acts of aiding under conditions of modern digital technologies are not only geographically unrestricted but also global in nature. This underscores the importance of international cooperation and global response mechanisms for detecting and suppressing such acts, regardless of where they occur.

Informational and media aiding constitutes a crucial component of contemporary military and hybrid conflicts and has gained increasing importance in the context of information warfare. It includes propaganda, media manipulation, and activities within social networks that enhance the aggressor's legitimacy and public support while discrediting its opponents.

This phenomenon extends beyond traditional mass media such as television and radio to encompass new media, particularly the Internet, where the dissemination of disinformation, fake news, and misleading narratives can significantly influence public opinion and shape perceptions of reality.

Investigating this form of aiding requires a comprehensive analysis of the content and quality of publications, identification of information sources, and the establishment of links between media structures engaged in such activities and the aggressor state. This approach allows for the construction of an objective picture of how media may function as instruments for spreading aggressive narratives.

For instance, during Russia's war against Ukraine, the extensive use of false narratives by Russian state-controlled and pro-Russian media platforms—such as claims about “Nazis” in Ukraine—contributed to the dehumanization of Ukrainians and the construction of an enemy image in public consciousness (Shlapachenko, 2023).

Within the context of information warfare, particular attention should also be paid to social media platforms, which have become key spaces for manipulation and propaganda. Platforms such as Twitter (X), Facebook, TikTok, and Telegram are actively used for agitation, where automated bots, fake accounts, and coordinated propaganda campaigns facilitate the creation and dissemination of myths and false narratives beneficial to the aggressor. Investigating this aspect requires meticulous analysis of information flows, their sources, and temporal dissemination patterns.

Concrete examples illustrate the forms and impact of aiding an aggressor state. For instance, in 2022, pro-Russian media disseminated false news on social networks about so-called “Ukrainian offensives” in the Donbas region. They also circulated narratives claiming that “Ukrainian nationalists” were destroying civilian populations during hostilities in eastern Ukraine. Propaganda campaigns organized through Telegram channels attempted to convince foreign audiences that the war in Ukraine was a “civil conflict” without external aggression, while Wikipedia was sometimes used to smear Ukrainian nationalists and patriots.

Military and technical assistance—including the provision of weapons, high-tech equipment, or training for the aggressor's armed forces—requires investigations far beyond simple monitoring of deliveries or contracts. Effective analysis demands a comprehensive study of networks connecting arms manufacturers, contractors, and the aggressor state. Supply chains may be both direct and indirect, passing through intermediary companies that use informal channels for transactions (Shvets, 2025).

Special attention should be given to the key actors involved in weapons and technology transfers, including state-owned enterprises, private companies, and shell structures hiding behind civilian contracts. Challenges arise when transactions occur through informal channels, making them difficult to trace—for example, arms deliveries disguised as humanitarian aid, a frequent occurrence in various conflict zones (Dopiriak; Zahyney-Zabolotenko, 2024).

Even thorough formal agreement analysis may fail to reveal how and through whom technical or military equipment is transferred. Traditional investigative methods are often inadequate, especially for international schemes where participants may change registration countries, use offshore entities, or shell companies to conceal their intentions.

Modern analytical approaches, such as big data analytics, are increasingly used to track financial flows and uncover hidden links among participants, even when they attempt to obscure their actions through complex intermediary chains. Blockchain monitoring, social media surveillance, and transaction analytics can reveal missing links and identify the actual beneficiaries of illicit transfers.

International cooperation is essential, as perpetrators may operate globally, exploiting multiple jurisdictions to evade accountability. Successful investigations depend on the coordination of law enforcement and intelligence agencies, as well as state collaboration to detect and disrupt these criminal networks. Such approaches enhance transparency in international security policy while blocking channels of weapons and technical assistance. (Dudorov; Movchan, 2022)

The technologies supporting aggression may include not only weapons but also cyberattack systems, communication networks, and other components that enhance military effectiveness. This raises not only moral and legal responsibility but also global security concerns, as providing technical assistance to an aggressor can create threats for other states, especially in the digital and automated era. (Mishchuk, 2023)

Intelligence sharing represents one of the most dangerous forms of aiding, with critical implications for national security. If such information reaches the aggressor or its agents, it may be used to conduct precision strikes against key infrastructure, military units, or civilians. Intelligence may

include military positions, tactical operations, or technical data essential for operational planning. Proper protection of such information is paramount.

Data can be transmitted through secure channels used for intelligence exchange between states or individuals. Those with access may, intentionally or negligently, transfer information to the aggressor or its agents, facilitating targeted attacks. Civilian intermediaries or shell organizations can further complicate accountability, intentionally or inadvertently supporting strategic objectives of the aggressor.

For example, agents or employees of foreign corporations with access to defense secrets can significantly strengthen the aggressor's targeting capabilities. Cyberattacks may also extract sensitive data from military networks for precision strikes. Information on technical processes, systems, and equipment crucial for military operations allows the aggressor to monitor adversary positions and conduct high-precision attacks on energy or transport infrastructure.

In a globalized world, cyber-mediated intelligence transfer has become widespread. Perpetrators may target military and governmental systems to extract classified data (Politova; Lehunova, 2025) Intelligence collection on strategic military objects or defense plans can facilitate sabotage and threats to national security. Providing access to strategically significant information to an aggressor or its agents constitutes one of the most dangerous forms of aiding. Strategic data may include troop locations, critical infrastructure, and essential national security systems.

Access to technical processes, such as the development of new defense technologies or management systems, is especially critical for a state's defense. If an aggressor obtains such data, it can not only monitor forces but also conduct precision strikes on vulnerabilities with maximum effect (Mokina, 2023)

The information in question may include not only the locations of military units but also detailed data on the placement of strategic facilities, such as ammunition depots, command posts, and key infrastructure elements essential for the functioning of the defense system. Moreover, strategically important information may not be limited to documents or digital archives; it can also include technical assets such as software, algorithms, or data on technical processes used in the development or maintenance of military systems. Loss of control over such data can significantly weaken a country's defense capabilities, as it enables an aggressor to conduct targeted strikes on the most vulnerable sites, potentially affecting the course of military operations.

Access to this information provides the enemy with substantial advantages, allowing not only physical attacks on infrastructure but also the development of complex strategies to deceive or disrupt defense systems, thereby undermining national security. Another critical aspect is the provision of materials, equipment, or technical components that can directly or indirectly enhance the aggressor's defensive or offensive capabilities. Such support includes equipment for weapons production or storage and technical components that facilitate military operations, threatening not only Ukraine's security but regional stability.

Actions aimed at collecting or delivering information, processes, objects, or documents to the aggressor state or its agents can harm national interests. This may include selling or providing intellectual property, technologies, or processes potentially usable for aggression, such as improving military technologies or intelligence capabilities. The destruction or damage of documents containing critical national security information can prevent the proper acquisition or use of necessary data for defense, substantially weakening the state during wartime.

One of the most dangerous forms of aiding the aggressor is active participation in separatist movements or contributing to the destabilization of Ukraine. Such activity may involve building barricades, trenches, and other fortifications to slow or impede Ukrainian forces, allowing the aggressor to advance or maintain territorial control. These fortifications reduce the operational capacity of the Armed Forces of Ukraine and strengthen enemy positions, delaying strategic progress and providing the aggressor more time to consolidate or plan further attacks (Mokina, 2023).

Participation in hostilities against government forces or direct support for such movements constitutes an even clearer form of aiding, as it directly spreads violence and aggression within Ukraine, undermining sovereignty and stability, worsening the humanitarian situation, and endangering civilians. Another severe form of aiding includes participation in open military occupation or actions aimed at destroying critical infrastructure essential for state functioning, particularly during war. Sabotage acts—such as destroying bridges, roads, energy facilities, or other strategic infrastructure—create systemic destabilization, disrupt military operations, complicate logistics, and reduce operational efficiency, directly affecting battles and strategic advances.

This category also includes facilitating disruptions in key government services and enterprises crucial for defense. For instance, sabotage targeting production facilities of weapons or military equipment strikes directly at the nation's ability to resist. Interruptions in energy and communications networks, along with other forms of economic sabotage, can significantly weaken national defense, producing strategic consequences during armed conflict (Dopiriak; Zahaney-Zabolotenko, 2024)

Participation in such actions not only violates national interests but actively contributes to long-term weakening of the country's defense potential, providing the aggressor with opportunities for further attacks and destabilization at all levels.

Attention should be given to methods of intimidating civilians in occupied territories. This approach aims not only at physical or psychological violence but also at deeply demoralizing citizens to undermine their support for state authorities. Threats, repression, torture, and overt terror create an atmosphere of fear and hopelessness among civilians, forcing adaptation to the occupier's reality, even if it means supporting the occupation. Such terror causes physical and moral suffering while systematically eroding the resilience of local communities.

Perpetrators of these methods manipulate civilians' emotions, exploiting fear, uncertainty, and anxiety that often accompany wars or crises. In such situations, people act under the influence of their greatest concerns—the safety of their families and their own lives—creating opportunities for manipulation. Emotional manipulation can drive certain population groups to participate in acts of aiding the aggressor, collaborate with the enemy, or even support sabotage and terror. This adds complexity to law enforcement efforts, as combating this phenomenon extends beyond addressing specific criminals, requiring society to develop psychological resilience and the capacity to resist manipulation.

An integral part of this situation is the importance of establishing national programs aimed at enhancing the psychological readiness of the population to act in crisis situations, teaching individuals to recognize manipulations and emotional tactics intended to weaken their morale. Education and support for citizens' mental health should become essential components of the national security system.

Thus, aiding an aggressor state takes many forms, ranging from active measures aimed at destroying or weakening Ukraine's defense capabilities to less obvious forms of assistance, such as sharing intelligence or providing resources for military operations. Together, these elements form a complex picture with multiple components, collectively posing a serious threat to Ukraine's national security and independence.

Acts of aiding an aggressor extend far beyond legal analysis, as they not only violate the law but also touch upon deeper social and moral dimensions. Responses to such crimes should be based not only on legal norms and sanctions but also on human and social considerations, given that these phenomena have far-reaching consequences for public morality, the mental state of the population, and the social fabric of society. Therefore, addressing such actions requires a comprehensive approach, which considers not only legal aspects but also sociocultural factors, the psychological impact on people, and the overall strategy for societal response (Shlapachenko, 2023).

Fair punishment for acts of aiding is essential to protect fundamental rights and state stability. However, it is equally important to develop a deeper understanding of these crimes, since in many cases aiding an aggressor is not merely a legal violation but also a breach of fundamental moral order,

social relations, mutual respect, and trust. For this reason, beyond criminal sanctions, efforts should focus on social-psychological mechanisms to prevent such acts.

Ensuring individual rights is crucial, but legal protection alone is insufficient to resolve deep social contradictions. It must be recognized that acts of aiding can contribute to the formation of hierarchies among people, where some are perceived as inferior, threatening, or “secondary,” while others are seen as legitimate representatives of authority or power. This can lead to social fragmentation, where a significant part of the population loses trust in state institutions, and another part loses trust in fellow citizens.

In this context, it is extremely important to preserve societal unity, foster a sense of shared responsibility for national interests and security, and cultivate national solidarity based on mutual respect, support, and the ability to compromise in challenging situations. Violations of this unity through acts of aiding create not only legal but also moral and ethical chasms within society.

Thus, combating acts of aiding must be multifaceted, incorporating legal, social, psychological, and ethical dimensions. This approach allows for effective responses to crimes while reducing the risk of recurrence, restoring and strengthening the foundations of social cohesion and national security (Dudorov; Movchan, 2022)

Classical criminology provides the epistemological basis for theorizing a general legal crime, which violates social and/or legal norms of a given society. Actors—criminals, victims, and law enforcers—can be identified, roles assigned, and legal means of protection are known. Acts qualifying as criminal offenses, along with their victims, are generally considered unique cases. The context in which these crimes occur is stable, and the principles of the rule of law ensure the protection of rights and the rendering of verdicts by a third party. Legal remedies exist to ensure justice, protect human rights in judicial proceedings, obtain compensation, and provide psychological and social support as well as reintegration into society after serving a sentence or recovering from victimization.

Conclusion. Aiding an aggressor state manifest in numerous forms, including financial, technical, informational, political, intelligence-related, and participation in destabilizing or separatist activities. Each form can significantly affect the state’s defense capability and population security. In today’s globalized and digitalized environment, geographical boundaries no longer limit acts of aiding, as international financial networks, the internet, social media, and digital platforms create new risks for the spread of aggression.

Counteracting such actions requires combining criminal-legal, socio-psychological, and technological approaches, including investigating financial flows, controlling the transfer of strategic and intelligence information, analyzing media and digital communication channels, and enhancing the population’s psychological resilience. A clear distinction between collaboration and aiding supports fair law enforcement, the protection of national interests, and adherence to the rule of law, all of which are critical for ensuring state stability and societal security.

References:

1. Dopiriak B. P., Zahynei-Zabolotenko Z. A. (2024). Formy umysnykh dii, spriamovanykh na dopomohu derzhavi-ahresoru (posibnytstvo), v sudovii praktytsi [Forms of intentional actions aimed at assisting the aggressor state (aiding) in judicial practice]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo*. Vol. 3. No. 84. Section 8: Criminal law and criminology; penal law. pp. 301–310. [in Ukrainian]
2. Dudorov O. O., Movchan R. O. (2022). Vidpovidalnist za posobnytstvo derzhavi-ahresoru: problemy kvalifikatsii ta vdoskonalennia kryminalnoho zakonu [Liability for aiding the aggressor state: problems of qualification and improvement of criminal law]. *Visnyk asotsiatsii kryminalnoho prava Ukrainy*. Vol. 2, No. 18. pp. 95–117. [in Ukrainian]
3. Mishchuk M. (2023). Osoblyvosti vidpovidalnosti za kryminalni pravoporushennia pid chas voiennoho stanu v Ukraini: ohliad zakonodavstva 2022–2023 rokiv [Peculiarities of liability for criminal

- offenses during martial law in Ukraine: a review of legislation of 2022–2023]. *Vyshehradskiy zhurnal z prav liudyny*. No. 5. pp. 34–45. DOI: 10.61345/1339-7915.2023.5.5. [in Ukrainian]
4. Mokina I. (2023). Kryminalna vidpovidalnist za kolaboratsiinu diialnist ta posobnytstvo derzhavi-ahresoru [Criminal liability for collaboration activities and aiding the aggressor state]. Available at: <https://www.hsa.org.ua/blog/kryminalna-vidpovidalnist-za-kolaboraciinu-diialnist-ta-posobnytstvo-derzhavi-agresoru> (Accessed: 08 January 2026). [in Ukrainian]
 5. Orzhynska E. I., Senina V. O. (2022). Posibnytstvo derzhavi-ahresoru: vzaiemozviazok mizh sposobom vchynennia ta osoboju zlochintsia [Aiding the aggressor state: the relationship between the method of commission and the perpetrator]. *Pivdenoukrainskyi pravnychi chasopys*. No. 4, Vol. 2. p. 102. [in Ukrainian]
 6. Politova A. S., Lehyhova N. O. (2025). Teoretyko-pravovi problemy kryminalnoi vidpovidalnosti za posibnytstvo derzhavi-ahresoru [Theoretical and legal problems of criminal liability for aiding the aggressor state]. *Analychno-porivnialne pravoznavstvo*. Vol. 3. No. 6. pp. 91–98. [in Ukrainian]
 7. Shlapachenko V. (2023). Problemni pytannia kryminalizatsii posibnytstva derzhavi-ahresoru (st. 111-2 KK Ukrainy) [Problematic issues of criminalization of aiding the aggressor state (Art. 111-2 of the Criminal Code of Ukraine)]. *Visnyk kryminalnoho sudochynstva*. No. 1–2. pp. 164–172. DOI: 10.17721/2413-5372.2023.1-2/164-172. [in Ukrainian]
 8. Shvets Yu. V. (2025). Materialno-resursna kolaboratsiia ta posibnytstvo derzhavi-ahresoru yak formy zlochynnoho obihu aktyviv: osoblyvosti skladiv zlochyniv i problemy kvalifikatsii [Material and resource collaboration and aiding the aggressor state as forms of criminal asset circulation: features of crime elements and qualification problems]. *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav – Bulletin of KhNUA*. No. 4 (111). pp. 270–282. DOI: 10.32631/v.2025.4.21. [in Ukrainian]