Check for updates

DOI: https://doi.org/10.34069/AI/2024.84.12.7

How to Cite:
Khoronovskyi, O., Orlean, A., Kostenko, I., Melnyk, O., & Sokiran, M. (2024). Threats to critical infrastructure: A study of transnational organized crime in Ukraine. *Amazonia Investiga*, *13*(84), 118-130. https://doi.org/10.34069/AI/2024.84.12.7

Threats to critical infrastructure: A study of transnational organized crime in Ukraine

Загрози об'єктам критичної інфраструктури: дослідження транснаціональної організованої злочинності в Україні

Received: November 2, 2024 Accepted: December 29, 2024

Written by:
Oleg Khoronovskyi[1]
https://orcid.org/0000-0001-9448-1180
Andriy Orlean[2]
https://orcid.org/0000-0002-7439-5311
Inesa Kostenko[3]
https://orcid.org/0000-0002-8784-5422
Oksana Melnyk[4]
https://orcid.org/0000-0003-1805-830X
Maksym Sokiran[5]
https://orcid.org/0000-0002-1682-2012

Abstract

The purpose of the article is to study the nature and content of threats to critical infrastructure facilities related to the activities of transnational organized criminal groups. In the course of the research, the following scientific methods were used: historical, monographic, logical, dogmatic, normative analyses, system and structural, legal modelling, prognostic, summarization. The conceptual apparatus and criteria for classification of threats to state security, proposed in the scientific literature and relevant legal instruments are considered. The authors' definition of the concept of "threats to critical infrastructure facilities related to the activities of transnational organized criminal groups" is proposed. The threats to critical infrastructure facilities related to the activities of transnational organized criminal

Анотація

Метою статті є дослідження сутності та змісту загроз об'єктам критичної інфраструктури, пов'язаних з діяльністю транснаціональних організованих злочинних угрупувань. У ході дослідження використовувалися такі наукові методи: історичний, монографічний, логічний, догматичний, нормативного аналізу, системно-структурний, правового моделювання, прогностичний, узагальнення. Розглянуто понятійний апарат та критерії класифікацій загроз державній безпеці в науковій літературі та нормативно-правових актах. Запропоновано дефініцію поняття «загрози об'єктам критичної інфраструктури, пов'язані з діяльністю транснаціональних організованих злочинних угрупувань». Також, авторами виокремлено загрози об'єктам критичної інфраструктури (за

[1] Candidate of Legal Sciences, Doctoral Student of the National Academy of the State Security Service of Ukraine (Kyiv, Ukraine). WoS Researcher ID: LZI-0947-2025 - Email: oleghor@ukr.net
[2] Doctor of Legal Sciences, Associate Professor, Professor of the Department of Criminal Law and Criminology of the Educational and Scientific Institute of Law and Psychology, National Academy of Internal Affairs (Kyiv, Ukraine). WoS Researcher ID: MDT-0258-2025 - Email: balansandrey@gmail.com
[3] Ph.D. in Law, Fellow Researcher at the University of Leicester (Leicester, United Kingdom), Researcher at the Research Institute of State Building and Local Self-Government of the National Academy of Legal Sciences of Ukraine (Kharkiv, Ukraine). WoS Researcher ID: ABH-4602-2020 - Email: kostenko.inesa@outlook.com
[4] Candidate of Legal Sciences, Associate Professor, Associate Professor of the Criminal Procedure Department, National Academy of Internal Affairs (Kyiv, Ukraine). WoS Researcher ID: KBW-4666-2024 - Email: melnik-oxana@ukr.net
[5] Ph.D. in Law, Lawyer, Scientific Institute of Public Law (Kyiv, Ukraine). WoS Researcher ID: LZI-5275-2025 - Email: maxim.sokiran@gmail.com

groups (according to the manifestation of the source of threat) are highlighted. Further prospective lines of research are indicated.

Keywords: cyberattacks, critical infrastructure, State security, threats to critical infrastructure facilities, transnational organized crime, transnational organized criminal groups.

проявом джерела загрози), пов'язані з діяльністю транснаціональних організованих злочинних угрупувань. Визначено подальші перспективні напрямки досліджень.

Ключові слова: кібератаки, критична інфраструктура, державна безпека, загрози об'єктам критичної інфраструктури, транснаціональна організована злочинність, транснаціональні організовані злочинні угрупування.

Introduction

The modern legal policy of Ukraine in the field of combating crime is in a state of radical transformations and reforms, which are designed to ensure maximum observance of human rights and freedoms and bring Ukraine closer to the EU integration. However, due to objective and subjective miscalculations during the implementation of large-scale reforms, the war of the Russian Federation against Ukraine, tensions in the international political arena, a sharp increase in the threats of terrorist attacks, there is a significant intensification of criminal processes and acquisition of new systemic quality by crime. Nowadays, organized crime is becoming a significant factor in increasing social tension and destabilizing social relations in all spheres of life, hinders the recovery of the economy, and slows down the integration processes of Ukraine's entry into the world community. The transnational and, unfortunately, "universal" nature of criminalization of social relations requires including transnational organized crime in the signs of the global crisis of human society in the 21st century and in the list of global threats to international, national and regional security of mankind.

The analysis of available sources of information indicates that transnational organized criminal groups can control a significant part of the shadow economy, introduce new illegal financial schemes related to the legalization (laundering) of proceeds from crime, including financing terrorist activities of the Russian Federation, evading international sanctions, transferring costs to temporarily occupied territories of Ukraine, etc. The activities of transnational organized criminal groups are characterized by a high level of organization and intelligence, qualified personnel, using the latest technologies of covert communication, stable corruption and international ties, etc.

This problem is extremely urgent for our country since due to the full-scale invasion of the Russian Federation, the destruction of a significant part of industrial facilities, agricultural sector, transport and logistics infrastructure, closure of significant part of the sales markets for Ukrainian producers, as well as the blocking of transit to third countries, its critical infrastructure is in a difficult situation, which creates a favorable basis for the penetration of transnational criminal groups into State authorities of various levels, the national economy, politics and threatens the sustainable development of the State. This leads to constant threats to critical infrastructure facilities, which are integrated into social processes and acquire permanent character.

Therefore, the issue of eradicating and preventing such processes becomes a priority direction of state policy in the security sector, acquires extraordinary relevance in today's conditions and is the subject matter of close attention from law enforcement agencies, scientists and the public. The awareness of global threat to critical infrastructure posed by the activities of transnational organized crime groups, and the emergence of problems associated with the need to combat them, has necessitated the scientific understanding of this issue.

Consequently, the purpose of the study is to develop the concept of "threats to critical infrastructure facilities associated with the activities of transnational organized criminal groups", as well as to identify the most common threats to critical infrastructure facilities, the source of which may be the activities of transnational organized criminal groups.

To achieve this aim, the following tasks should be solved:

1) To consider certain aspects of the genesis and manifestation of this type of crime as a source of threat through the prism of ensuring State security;
2) To examine the concept of threat (within the issue of critical infrastructure sector) in the works by domestic scientists and the approaches to this term in some foreign countries (the US, Germany, the UK);
3) To investigate the approaches to the definition “threats to critical infrastructure facilities” enshrined in relevant legal instruments of Ukraine;
4) To learn scientific views on the classification of threats to critical infrastructure facilities and to propose the authors’ classification according to the manifestation of the source of threat;
5) To formulate the concept of "threats to critical infrastructure facilities associated with the activities of transnational organized criminal groups";
6) To make respective conclusions and to outline future lines of research based on the results of the study.

Methodology

Scientific methods are the basis of any research, helping to ensure the objectivity and reliability of the results obtained. Each method has its own specifics, due to which we can study various aspects of the chosen topic in more depth. The chosen methods helped to structure the research process, determine the stages and order of tasks, ensure the reliability and authenticity of the results, which makes it possible to implement the research results into practical application and use them in real conditions.

The methodological basis for the research is a system of general and special scientific methods and approaches, ensuring the objectivity of the study and complete exploration of the subject matter of the work. Taking into account the specifics of the research topic, the following methods were used:

Historical method was used to investigate the genesis of transnational organized criminal groups formation and manifestation of this type of crime as a source of threat through the prism of ensuring State security.

Monographic, logical and dogmatic methods contributed to the examination of the concept of threat (within the issue of critical infrastructure sector) in the works by domestic scientists and the approaches to this term in some foreign countries (the US, Germany, the UK).

Comparative and legal method was chosen for the comparison of the approaches to critical infrastructure protection in leading European States (Germany, Poland, Slovakia, Israel).

The method of normative analyses, as well as interpreting method helped to investigate the approaches to the definition of “threats to critical infrastructure facilities” enshrined in relevant legal instruments of Ukraine.

System and structural and systemic methods were applied for considering scientific views on the classification of threats to critical infrastructure facilities and formulating the authors’ classification according to the manifestation of the source of threat.

Legal modelling method made it possible to formulate the Authors’ definition of "threats to critical infrastructure facilities associated with the activities of transnational organized criminal groups".

Prognostic as well as summarization methods were helpful when making respective conclusions, discussing the implications of the findings for theory and practice and suggesting future lines of research.

Limitations in the choice of scientific research methods are determined by the purpose of the research (to develop the concept of "threats to critical infrastructure facilities associated with the activities of transnational organized criminal groups", as well as to identify the most common threats to critical infrastructure facilities), the specificity of the object (activities of transnational organized criminal groups to the detriment of critical infrastructure facilities), available resources (available works by foreign and domestic scholars, current legal instruments on the issue under consideration, publicly available data bases), and scientific ethics (methods should avoid subjectivity, falsification, or manipulation of data).

Literature review

A number of foreign and domestic authors have dedicated their works to the issue of transnational organized crime. For example, J. Anderson Black (1992) examined this global phenomenon starting from emerging of Mafia in Sicily, Yakuza in Japan, Triads in Chine and Mafia in post-Soviet Russia. However, states the Author, nowadays organized crime has gone international, and North America, Europe, Australia, and Southeast Asia are suffering because of this terrible phenomenon.

According to Shelley (2005), whose view we completely support, transnational organized crime is not a homogeneous phenomenon given that its structural units can form and develop in different political and economic conditions. All these structures exploit weaknesses in national and international law enforcement systems, differences in the rules of banking, investment, criminal and other branches of law. At the same time, there is no form of government with permanent immunity to transnational organized crime in the modern world, as well as there is any political and legal system that would be able to exercise total control over its functioning, any financial or economic system that would be able to put an end to the illegal activities of transnational criminals.

Transnational forms of organized crime were considered by Williams (2001), who believes that transnational organized crime is a new factor in geopolitics with its own character and logic of development. The scientist emphasizes, first of all, the economic essence of the phenomenon, but also defines the political aspects of its functioning. He actually equates a part of powerful transnational criminal organizations with legal transnational corporations, whose only difference from transnational criminal organization is nature and forms of capital accumulation and circulation.

As for the modern Ukrainian doctrine, the problems of scientific development of transnational organized crime in the spheres of economic activity that may be related to the critical infrastructure activities, were considered in a number of works.

Bobro (2015) proposed to consider threats to critical infrastructure as existing and potentially possible phenomena and factors that pose a danger to the sustainable functioning of critical infrastructure facilities. He focuses on man-made accidents and technical failures, often caused by human error, natural disasters and malicious actions.

Biriukov et al. carried out (2015) a comprehensive analysis of threats related to accidents, dangerous natural phenomena and malicious actions. They emphasized the need for a systemic approach to protecting critical infrastructure, taking into account both traditional and new challenges.

Sukhodolia (2016) identified key threats to critical infrastructure, such as emergency situations (natural disasters and man-made accidents), terrorist acts, sabotage and cyber threats. He draws attention to their growing complexity and frequency, which emphasizes the need for an integrated approach to their prevention and minimization.

Herasymenko (2024) analyzed the threats to Ukraine's critical infrastructure. Having based on international and domestic experience, the scholar classified them into: physical assaults, cyberattacks, economic sabotage, terrorist actions, and assaults using climate weapons. He states that this classification allows for a more accurate risk assessment and the implementation of appropriate measures to protect national critical infrastructure facilities.

As Biriukov et al. (2015) correctly point out, the tense military and political situation, in which our state defends its own territorial integrity and sovereignty, is characterized by a significant increase in the level of such threats of malicious actions as the commission of terrorist acts and sabotage operations on the territory of our country, directed at critical infrastructure facilities. Clearly, the most serious is potential threat of using nuclear energy facilities for terrorist purposes. There is also significant increase in the intensity of cyberattacks on the information and telecommunications infrastructure in Ukraine. Cyberattacks via the Internet are experienced by servers of state institutions, large companies, financial institutions, political parties and the media, as well as the information and telecommunications infrastructure of military facilities.

It can be stated that the works of these scientists are of great importance for legal science in the field of transnational organized crime research. At the same time, it should be noted that until now neither a generally accepted understanding of threats to critical infrastructure facilities, including those related to the activities of transnational organized criminal groups, nor their place in the state security system has been clearly defined, which determined the relevance of our research.

Results and discussion

First of all, it is worth to refer to the genesis of transnational organized criminal groups formation and manifestation of this type of crime as a source of threat through the prism of ensuring State security, as it is the pre-condition for understanding the features and specifics of its functioning nowadays, i.e. on the territory of Ukraine.

Thus, in domestic criminology, it is traditional to believe that the roots of modern transnational organized crime in the economic sphere go back to Soviet times, when in the 1960s and 1980s, the unfavorable economic situation led to negative quantitative and qualitative changes in crime. The proportion of crimes in the economy increased, material damage from them increased in many times. Due to the relaxation of law enforcement control, there was the rise of large-scale thieves of socialist property; shady businessmen (traders) with corrupt representatives of the party and state apparatuses began to operate – and all of them had been criminally enabled to make a profit. In fact, in the last decades of the Soviet system, a powerful layer of economic criminality was created, which significantly grew and enriched during the period of restructuring and redistribution of property (Kornienko, 2004, p. 8).

Then, in the late 1980s and early 1990s, there was a process of first confrontation, and the merger of black economy traders with criminal groups of a traditional general criminal orientation. The active consolidation of criminal groups has gradually led to their establishment of control over entire branches of trade, production, transport, small, medium and large entrepreneurship, financial operations. Starting from the 90s, the spread of negative processes was facilitated by such factors as the imperfection of the domestic legal framework regulating relations in the sphere of economy and public administration, a large number of unemployed and low-income sections of the population that became a potential pool of human resources for various criminal (including organized) groups. Gradually, at the end of the first half of the 90s, organized criminal groups began to form on the basis of a kind of alliance representatives of the administrative and economic nomenclature, businessmen from the economy and criminality. Subsequently, this union acquired a permanent and systemic character (Burkal, 2019, p. 9).

With the collapse of the USSR, the previously unified legal space narrowed to the territory of individual new States. At the same time, the criminal space not only did not narrow, but also preserved its previously shared territory.

In the future, the processes of democratization of society, the fall of the “Iron Curtain”, the weakening of border control, the liberalization of foreign economic activity, became a catalyst for the integration of domestic organized crime into the world criminal community. Gradually, domestic organized crime began to acquire characteristics of transnational one. Other factors of the rapid spread of transnational organized crime in Ukraine were the crisis socio-political situation, the presence of significant gaps in criminal, criminal procedural, customs, and economic legislation, the lack of effective methodological developments on countering the new socially dangerous phenomenon, and an imperfect mechanism of interstate coordination.

Over time, organized criminal groups went far beyond the territory of the State, establishing ties both with criminal structures and with legally operating economic entities. Their material, technical and financial base was strengthened, professionalism, organization and interaction with similar structures abroad enhanced. The spread of transnational ties of organized criminal groups was also facilitated by the central geographical location of Ukraine, the longest border length in Europe (8,215 km), which, in combination with complex socio-economic processes both in our country and in neighboring States, led to the country falling into one of the epicenters of transnational criminal flows.

According to the researchers, the features of the internationalization of post-Soviet organized crime were: high rates of migration processes on the territory of the CIS; the powerful financial resources of post-Soviet crime, resulting from the unprecedented plunder of national wealth in the CIS countries, enabled it to carry

out extensive investment activities in different regions of the world; the integration of organized crime with political regimes in many CIS countries, which led to the transformation of the territory of the Commonwealth into a haven for criminal structures (Doroshenko, 2003, p. 20). In general, approximately by the mid of the 2000s, the activities of transnational organized criminal groups acquired a modern appearance, covering such areas of the economy as: credit and finance, banking, privatization, real estate, the stock market, virtual assets, foreign economic activity, and others (Sukhodolia, 2016).

At the current stage, the determining factors of forming threats to critical infrastructure facilities related to the activities of transnational organized criminal groups are globalization processes taking place in the world community, namely: development of international relations, creation of transnational corporations, simplification of procedures for crossing state borders, unification of international public organizations, introduction of international payment systems, etc. The UN report "The globalization of Crime: A transnational organized crime threat assessment" states that criminal organizations earn billions of dollars annually from trafficking in drugs, weapons, people, raw materials, counterfeit products, as well as maritime piracy and cybercrime, but this threat concerns not only the economy. Income from criminal activity and the threat of the use of force allow criminals to influence elections, politicians and the military, and the largest economies become vast markets for illicit goods (UNODC, 2010).

It is worth additionally noting that significant destabilizing factors in Ukraine related to the activities of transnational organized criminal groups are: criminalization of the sphere of economic relations (illegal transactions in external investment and credit channels, attempts to establish control over profitable entities of economic activity, transport and communication); illegal operations with financial resources (fraud, transfer of funds abroad using forged documents; legalizing, laundering proceeds of crime); fraud using ultra-new means of payment and computers, etc. No less important factors, in our opinion, are internal processes, in particular, instability of the government and political system, functioning of various oligarchic groups of influence, imperfection of the current legislation, constant reformation of law enforcement agencies, temporary occupation of part of the territory of Ukraine by the Russian Federation, etc.

Summing up, we can highlight the main internal and external factors shaping the threats to critical infrastructure facilities related to the activities of transnational organized crime groups, in particular:

Internal ones: unstable political situation; corruption vulnerability of the state apparatus, including the judicial branch of government; insufficient effectiveness of the law enforcement system; imperfection of the current legislation; slow pace of reform implementation; functioning of oligarchic groups of influence; low level of solvency of the population; large number of unemployed; low level of ensuring economic competition; monopoly-oriented economy;
External ones: war of the Russian Federation against Ukraine; temporary occupation of Ukrainian territories in the east and south of our country; intensification of intelligence-subversive, intelligence-sabotage, terrorist and other illegal attacks on critical infrastructure facilities using organized crime (including transnational one); formation of a global financial system, high speed of capital movement, ensuring international circulation proceeds from crime; development of a single global information network "Internet", leading to an increase in the number of computer crimes (criminals have gained the opportunity to interfere in trade and financial transactions, trade and financial transaction systems, hack accounts, credit card systems, etc.); integration of the transport and logical system, mobility of material and human resources; creation of offshore markets that are not taxed, which contributes to the export and legalization of criminal capital, etc.; different systems of criminalization and degree of responsibility; global financial crisis.

Having dealt with historical development of this phenomenon and evolution of external and internal factors shaping the threats to critical infrastructure facilities related to the activities of transnational organized crime groups, we turn to the basic concepts related to the subject matter of our research.

The modern explanatory dictionary of the Ukrainian language defines the term "threat" as the possibility, inevitability of danger (Busel, 2005). Yermoshenko & Horiacheva (2010), researching the problems of financial security of the State, states that a threat is a specific and immediate form of danger or a set of negative factors or conditions. Instead, Pekin (2007) offers a more extended definition of this concept as the most concrete and immediate form of danger, that is, an existing danger that is characterized by a specific form of manifestation by a means of influence or a set of conditions and factors creating danger to the interests of citizens, society and the State, as well as national values and the national way of life.

Hubskyi (2001) also refers to the features of danger as the factors that directly or in the future make it impossible or difficult to implement national economic interests, creating obstacles to the normal development of the economy, a danger to state independence and the well-being of the people.

In view of the above, it can be concluded that despite certain contradictions in the definition of the term "threat", the researchers call the possibility of creating real or potential danger as its defining feature, which we agree with.

Under the "threat" in the context of critical infrastructure protection Bobro (2015, p. 92) suggests understanding "existing and potentially possible phenomena and factors creating danger to the sustainable functioning of critical infrastructure facilities and may lead to negative consequences". We consider this definition quite objective, which may be confirmed by its almost identical wording in the Green Paper on a European programme for critical infrastructure protection, where this term means "any circumstances or events that may disrupt the sustainable functioning or destroy critical infrastructure or any of its element, as well as any attempts and intentions to harm critical assets" (Commission of the European Communities, 2005).

A similar standpoint is supported by Yermenchuk (2017), who believes that the threat to critical infrastructure facilities is "existing or potentially possible phenomena and factors that can harm such an object (physical or in cyberspace), render it inoperable or otherwise fail to function as intended what constitutes a danger to vital national interests of Ukraine".

In the USA, the threats to critical infrastructure are understood as natural or man-made phenomena, natural persons, actors or actions containing or bearing potential harm to life, information, operations, the environment and/or property (Telenyk, 2018, p. 365). It is worth noting that the term "critical infrastructure" first appeared in the PDD-63 directive (Presidential Decision Directive) (The White House, 1998), which was signed by the US President Bill Clinton. The said Directive classified critical infrastructure as a national vital interest, defined goals and formed a concept for reducing its vulnerability in the public and private sectors. And most importantly, it established a requirement to ensure the security of critical infrastructure elements.

Subsequently, the issue of critical infrastructure and its security began to evolve in European countries, in particular, Germany, Great Britain, the Netherlands, the Czech Republic, Slovakia, Poland, Hungary, etc. In Europe, the problem of critical infrastructure protecting was first addressed in Great Britain, 1999, by defining its main and the responsibility of certain state bodies for its protection. National critical infrastructure was defined as systems whose continuity is important for the functioning of the state, the loss or disruption of which would or could endanger the lives of citizens, could have serious negative economic or social consequences for society or a large part of it. Such systems included state administration, reserve services, energy and fuel supply, water supply, telecommunications, food supply, sanitation, finance and economics, communication networks and services, justice and protection of public order, social services, education, science and testing, weather forecasting, etc.

According to the UK legislation, threats can range from terrorism to attempts by states to harm people in the UK and undermine their way of life. From the beginning of the construction of the critical infrastructure protection system in the UK, attention was primarily paid to the need to protect against threats in the field of state security. Therefore, the National Infrastructure Security Coordinating Center (NISCC) and the National Security Advisory Center (NSAC) had been cooperating for a long time. Subsequently, the Center for the Protection of National Infrastructure (CPNI) was formed on their basis, which provides comprehensive security advice to enterprises and organizations that are operators of critical infrastructure, including information, personnel and technical aspects of security, helping to reduce the vulnerability of national critical infrastructure to terrorism and other threats. Subsequently, the functions of countering threats in the field of computer security were transferred to the National Cyber Security Center (NCSC). Ensuring the resilience of the UK in dealing with the emergencies and the corresponding threats is the responsibility of the Contingencies Secretariat (CCS), which facilitates the work of the Center for Crisis Management (COBR), which ensures the rapid development of a common position and the implementation of coordinated response to existing threats (Yermenchuk, 2017).

Among the European countries, it is useful to highlight the active identification and analysis of threats to critical infrastructure carried out by Germany. According to the National Strategy for Critical Infrastructure

Protection (CIP Strategy) (Federal Ministry of the Interior, 2009), the concept of threat is defined as the possibility of events (natural phenomena, technical failures or human mistakes, errors in human behavior) that can cause damage to persons, material values and the environment or lead to the disruption of social and economic relations.

In 2007, Slovakia adopted its first document on critical infrastructure protection, which defines a general strategy for protecting vital objects, but does not have a detailed plan of action in crisis situations. Critical infrastructure is defined as that part of the national infrastructure (selected organizations and institutions, objects, systems, equipment, service systems), the destruction or limitation of which as a result of the influence of risk factors will endanger or disrupt the political and economic course of the state or will threaten life and health of the population. Defense infrastructure objects are also an integral part of critical one. In 2011, the Law on Critical Infrastructure of the Slovak Republic, which clearly defines the critical infrastructure objects, the state bodies responsible for their protection, as well as a detailed plan of measures in case of an emergency, was adopted. This Law defines that critical infrastructure consists of elements, whose disruption or destruction would have serious adverse consequences for the performance of the economic and social functions of the state and, consequently, the quality of life, protection of life, health, safety, property and the environment. We can generalize that critical infrastructure includes physical objects, resources, services and information and communication technologies, networks and other infrastructure assets which, if disrupted or destroyed, would have serious consequences for the health, safety or economic well-being of citizens or the effective functioning of the State (Act No. 45/2011, 2011).

In Poland, critical infrastructure is defined as functionally interconnected means of production, institutions, and services that are key to the security of the country and its citizens in ensuring the proper functioning of both state and self-government bodies and institutions, and the commercial (private) sector. In 2007, the Polish government adopted the law on crisis management, within the framework of which a clear understanding of the parameters of critical infrastructure and their protection is presented (Law of Crisis Management, 2007).

In Israel, experts define infrastructure as critical if its disruption may lead to significant socio-economic shocks that are able to undermine stability in society and thereby lead to the threats to the country's national security. It is well known that the security system for airport terminals (one of the vulnerable critical infrastructure items) developed in Israel is nowadays the most effective one in the world (Hriniaiev, 2012).

At the same time, it should be noted that there is no legal definition of the concept of “threat to critical infrastructure facilities” in Ukraine, as well as there is any general approach to their classification. The Law of Ukraine “On the National Security of Ukraine” (Law No. 2469-VIII, 2018) provides the following definition of threats in the context of ensuring national security – these are phenomena, trends and factors that make impossible or complicate the realization of national interests and the preservation of national values of Ukraine.

The Decree of the President of Ukraine “On the National Security Strategy of Ukraine” (Decree No. 392/2020, 2020) defines current and projected threats to the national security and national interests of Ukraine, taking into account foreign policy and internal conditions. Having analyzed the provisions of the Decree, the following can be attributed to threats to critical infrastructure facilities in the context of countering transnational organized criminal groups:

- The modern model of globalization has enabled the spread of international crime, in particular in the legalizing (laundering) proceeds of crime;
- The inconsistency and incompleteness of reforms, as well as corruption hinder the recovery of the Ukrainian economy, make its sustainable and dynamic growth impossible, increase vulnerability to threats, and fuel the criminal environment;
- Insufficient protection of property rights, slow development of market relations in key areas, including the use of land and subsoil, significant role of the public sector in the economy, imperfection and fragmentation of legislation restrain economic growth, attraction of domestic and foreign investments;
- Insufficient level of competition and dominance of monopolies, in particular in the energy sector and infrastructure, low energy efficiency reduce Ukraine’s competitiveness, threaten the well-being of its citizens;
- The threats to critical infrastructure, related to the deterioration of its technical condition, the lack of investment in its renewal and development, unauthorized interference in its functioning (in particular,

physical and cyber), ongoing hostilities, as well as the temporary occupation of part of the territory of Ukraine, are constantly increasing.

It should be noted that any of the current and foreseeable threats defined by the Decree may have a direct or indirect impact on critical infrastructure facilities, and by their very nature to be considered a threat. At the same time, in this context, we in this context we have been based on the purely economic categories and their direct relation to critical infrastructure functioning.

The Strategy for Ensuring State Security also states that the threats to critical infrastructure related to the temporary occupation of a part of the territory of Ukraine, ongoing hybrid influences by the entities of intelligence-subversive activities, the deterioration of the technical condition of such infrastructure, and attempts to illegally interfere with its functioning, including physical and, in particular physical and cyber ones, are increasing (Decree No. 56/2022, 2022).

Interesting in terms of the problem under consideration is the Decree of the President of Ukraine "On the Strategy of Economic Security of Ukraine for the period up to 2025" (Decree No. 347/2021, 2021), which defines challenges and threats in the spheres of financial, production, foreign trade, investment and innovation, macroeconomic security. Having studied the provisions of this Decree, the following can be attributed to threats to critical infrastructure, which are in one or another way related to the activities of transnational organized criminal groups:

- High level of "shading" economy;
- Loss of budget revenues due to widespread phenomena of "grey" imports and smuggling, tax evasion schemes, tax base erosion through the use of "low-tax" jurisdictions;
- Inconsistency of legal regulation of relations in the tax sphere;
- The spread of the phenomenon of legalizing (laundering) proceeds of crime;
- Unsatisfactory technical condition and level of protection of critical infrastructure facilities, insufficient investment in its renewal and development, potential threat of unauthorized physical and cyber interventions in its functioning;
- Lack of favorable conditions for attracting investment and reinvestment, as well as insufficient institutional support for these processes;
- Insufficient level of protection of intellectual property rights;
- Illegal directions to domestic technological developments and innovations by foreign entities and the risks of their unauthorized leakage abroad;
- Low protection of property rights;
- Corruption.

Current legislation does not classify threats to critical infrastructure facilities either by criteria or spheres. In contrast, a number of criteria for the classification of threats in various spheres of life have been proposed in the scientific literature. The most widespread is location-based separation of threats into internal and external in relation to the security object. Accordingly, external threats arise in the object's external environment, while internal threats are determined by the state of the security object itself.

The classification and division of threats into real and potential ones is of great importance in the system of security sciences. Such a division is carried out according to the probability, by the risk level of conditions under which danger occurs. In case of potential threat, there is a possibility of some harm (damage), but its scale does not constitute danger. In the case of a real threat, significant harm (damage) is caused. If the potential threat must be prevented in order to avoid its negative impact, then a real threat requires an immediate response from state authorities in the form of specific measures to directly counter the threat to minimize its destructive impact on security and prevent it from turning into a real danger (Pyrozhenko, 2006, p. 25). In our opinion, the thesis "in the case of real threat, the harm is caused" is quite debatable, since harm can be inflicted only when the threat is implemented, that is, specific acts (actions or omission) aimed precisely at achieving the specified result.

There are also other classifications of threats in the scientific literature. Thus, by the degree of danger, it is customary to divide threats into particularly dangerous (with a maximum level of impact), dangerous (with an average level of impact) and potentially dangerous (with a minimum level of impact). Depending on the specifics of the occurrence of threats, they are divided by the suddenness and frequency of occurrence, as well as by the time of manifestation. According to the duration of the destructive impact, threats are

classified into systemic and additionally acquired. By the mechanism of influence, threats are divided into direct and indirect. According to the possibility of influence on threats and the sources of their occurrence, they are divided into controlled, which are influenced, and unmanaged, which are not influenced by the public authorities (Khylko, 2004).

As for threats to critical infrastructure facilities, it is proposed to divide them into three groups, which include accidents and technical failures, natural disasters and dangerous natural phenomena, malicious actions (by groups or individuals, such as terrorists, criminals and saboteurs, industrial espionage, as well as hostilities). Especially dangerous are combined threats and threats, the implementation of which can lead to disastrous and varied cascade effects due to the interdependence of critical infrastructure elements.

Threats from physical impact from the inside and outside of critical infrastructure facilities, threats arising from human miscalculations and technical failures, terrorism or criminal acts are also distinguished. An example of a threat from the inside of a facility is a so-called «intentional error», for example, the intentional incorrect programming of control systems, which leads to accidents or production stoppages, interference with important parts of the plant using the auxiliary means and tools available at any enterprise. External threats may include a vehicle accident, arson, use of explosives, shelling, plane crash, use of chemical, biological, radiological or nuclear weapons. Criminals can also apply combined actions (Yermenchuk, 2018).

As for the subject matter of our scientific research, the classifier of threats to critical infrastructure facilities is the manifestation of the source of threat, to which we refer for transnational activities organized criminal groups. We highlight the following threats to critical infrastructure facilities related to the activities of transnational organized criminal groups according to the criteria of manifestation of the source of threat:

- Introduction and implementation of illegal schemes and mechanisms in the course of privatization, public procurement, management of state corporate rights, bankruptcy of state enterprises, VAT administration, other operations affecting the operation of critical infrastructure facilities;
- Using administrative, financial and other resources of critical infrastructure facilities in the war of the Russian Federation against Ukraine;
- Corruption links in the authorities and administrations, facilitating the implementation of criminal schemes;
- Obtaining advantages in the field of public procurement, state benefits and other economically unjustifiable preferences by criminal entities at the expense of critical infrastructure facilities;
- Acquisition of Ukrainian intellectual property facilities, information containing commercial secrets and their use in the illegal activities to the detriment of critical infrastructure facilities;
- Receiving and using restricted information circulating on critical infrastructure facilities for criminal purposes;
- Lobbying for the adoption of legal acts for private purposes at the expense of critical infrastructure facilities;
- Transfer of capital, obtained as a result of activities to the detriment of critical infrastructure facilities abroad with the aim of tax evasion and legalization of criminal property in favorable jurisdictions;
- Reducing the investment attractiveness of critical infrastructure facilities and violation of healthy competition against them due to the application of «unfair» rules;
- Development and implementation of cyber disruptions to the detriment of critical infrastructure facilities by criminal entities;
- Containment of development in critical infrastructure sectors, non-improvement of legislation in the field of critical infrastructure protection.

This classification (according to the manifestation of the source of threat), in our opinion, allows solving a number of problems in the national system of critical infrastructure protection, namely:

1) Identifying any actor, phenomenon, event, process or set of conditions as a threat to critical infrastructure facilities, as well as classify it by characteristics, which allows planning, developing and implementing a set of measures to ensure effective functioning of critical infrastructure systems;
2) Involves the use of in the formation and clarification of the main goals and objectives in the field of operation and protection of critical infrastructure;

3) To be used in forecasting strategic directions of critical infrastructure supply, as it provides for the possibility of grouping threats according to the degree of danger as a result of a quantitative assessment of the level of negative impact on the provision of basic services in the event of destruction, damage or malfunctioning of critical infrastructure facilities;
4) Enables to abandon the traditional inclusion of a rather hypothetical list of threats to critical infrastructure facilities in national security regulations, without drawing a line between them on the essential signs of the origin and nature of the influence.

The presented threats to critical infrastructure facilities related to the activities of transnational organized criminal groups are not exhaustive – they depend on many subjective and objective factors, evolve and degrade due to the changes in social relations.

Summing up, we can conclude that the results of the study enabled to formulate a definition of the concept of "threats to critical infrastructure facilities related tothe activities of transnational organized criminal groups", as well as to define such them. Thus, we interpret this term as existing and potentially possible phenomena and factors arising in the process of activities of transnational organized criminal groups and are capable of hindering the stable operation of critical infrastructure facilities, lead to damage both to the object itself and to the State as a whole.

Conclusions

Summing up, we can conclude that the results of the study enabled to formulate a definition of the concept of "threats to critical infrastructure facilities related to the activities of transnational organized criminal groups", as well as to define such them. Thus, we interpret this term as existing and potentially possible phenomena and factors arising in the process of activities of transnational organized criminal groups and are capable of hindering the stable operation of critical infrastructure facilities, lead to damage both to the object itself and to the State as a whole.

The presented threats to critical infrastructure facilities related to the activities of transnational organized criminal groups (according to the manifestation of the source of threat) are not exhaustive – they depend on many subjective and objective factors, evolve and degrade due to the changes in social relations. It should be noted that in the modern conditions of the globalized world, organized crime of a transnational nature threatens not only the critical infrastructure of individual states, but also the international legal order in general, therefore the development and implementation of effective measures to counter this socially dangerous phenomenon should be declared as a priority direction of each country policy.

In our opinion, the proposed concepts and types of threats to critical infrastructure facilities, the source of which may be the activities of transnational organized criminal groups, will significantly contribute to:

- Orienting law enforcement to counteract the most significant threats to critical infrastructure facilities, without being distracted by minor ones;
- Clear understanding of the essence of the identified threats to critical infrastructure facilities, methods for their identification and elimination;
- Organizing large amounts of information on the activities of transnational organized criminal groups to the detriment of critical infrastructure facilities;
- Optimizing law enforcement activities through economy and rational deployment of forces and means;
- Identifying gaps and conflicts of laws, as well as the reasons and conditions contributing to the illegal activities of transnational organized criminal groups to the detriment of critical infrastructure facilities;
- Mastering techniques and methods of countering the activities of transnational organized crime groups to the detriment of critical infrastructure facilities.

Further prospective lines of research may include the study of threats to critical infrastructure facilities related to the activities of transnational organized crime groups in individual sectors of critical infrastructure, in particular: fuel and energy, food industry and agro-industrial complex, capital markets and organized commodity markets, finance, etc.

Bibliographic references

Act No. 45/2011. On Critical Infrastructure. *National Council of the Slovak Republic*, February 08, 2011. https://www.zakonypreludi.sk/zz/2011-45

Biriukov, D.S., Kondratov S.I., Nasvit O.I., & Sukhodolia O.M. (2015). *Green book on critical infrastructure protection in Ukraine: analytical report.* Kyiv: National Institute of Strategic Studies. https://niss.gov.ua/sites/default/files/2015-12/Green%20Paper%20-%20dopovid.pdf

Black, J. A. (1992). *Organized Crime*. Devon: Blitz Editions. https://www.amazon.com/Organized-Crime-J-Anderson-Black/dp/1856051110

Bobro, D. (2015). Determination of *assessment criteria and threats to critical infrastructure. Strategic priorities. Series*: Economy, 4, 83-93. https://acortar.link/Todbqv

Burkal, V. S. (2019). *Countering Transnational Organized Crime in the Economy* (PhD Dissertation). University of the State Fiscal Service of Ukraine. https://acortar.link/smEZS9

Busel, V. (2005). *A great dictionary of modern ukrainian language*. Kyiv, Irpin: Perun. https://acortar.link/AVToE4

Commission of the European Communities (2005). *Green Paper on a European program for critical infrastructure protection*. https://acortar.link/Q8PU4b

Decree No. 347/2021. On the Strategy of economic security of Ukraine for the period up to 2025. *President of Ukraine*, 2022. Retrieved from https://zakon.rada.gov.ua/laws/show/347/2021#Text

Decree No. 392/2020. On the decision of the National Security and Defense Council of Ukraine "On the National Security Strategy of Ukraine". *President of Ukraine*, 2020. Retrieved from https://www.president.gov.ua/documents/3922020-35037

Decree No. 56/2022. On the decision of the National Security and Defense Council of Ukraine "On the Strategy on ensuring State security". *President of Ukraine*, 2022. Retrieved from https://www.president.gov.ua/documents/562022-41377

Doroshenko, A. (2003). *Doroshenko. The factor of transnational crime in modern international relations*. (PhD Dissertation). Institute of World Economy and International Relations of the National Academy of Sciences of Ukraine. http://www.irbis-nbuv.gov.ua/aref/20081124053246

Federal Ministry of the Interior (2009). *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. https://acortar.link/mZEM3p

Herasymenko, O.M. (2024). Threats to critical infrastructure facilities of Ukraine under martial law. The collection of «Uzhhorod National University Herald. *Series: Law»*, *84*(3), 257-263. https://doi.org/10.24144/2307-3322.2024.84.3.39

Hriniaiev, S. (2012). *On the perspective on the issue of critical infrastructure security in the State of Israel*. Center for Strategic Assessments and Forecasts, May 22, 2012. https://acortar.link/eXxwSi

Hubskyi, B. (2001). *Economic security of Ukraine: measurement methodology, state and strategy of provision*: monograph. Kyiv: Ukrarchbudinform. ISBN 966-7521-15-X

Khylko, O. (2004). *Theoretic basis of identification of the threats to national security of Ukraine and the ways of its provision*. (Doctoral Dissertation). Taras Shevchenko National University of Kyiv. https://uacademic.info/ua/document/0404U004856

Kornienko, M. (2004). *Organized crime in Ukraine: current state, criminological characteristics, countermeasures*. Kyiv: Jurnauka Foundation. ISBN 996-96472-0-7

Law No. 2469-VIII. On the National Security of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*, dated June 21, 2018, No. 31, Art. 241. Url: https://zakon.rada.gov.ua/laws/show/2469-19#Text

Law of Crisis Management. *Chancellery of the Sejm*, dated April 26, 2007, No. 89, Art. 590. Url: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/T/D20070590L.pdf

Pekin, A. (2007). Economic security of enterprises as an economic and legal category. *Economist*, *8*, 23-25.

Pyrozhenko, V.A. (2006). Methodology of operationalization of basic concepts of national security: humanitarian component. *Political management, 3*, 21-34. https://acortar.link/GyeVZY

Shelley, L. (2005). The Unholy Trinity: Transnational Crime, Corruption, and Terrorism. *The Brown Journal of World Affairs, 11*(2), 101-111. https://www.jstor.org/stable/24590550

Sukhodolia, O.M. (2016). Protection of critical infrastructure in conditions of hybrid warfare: problems and priorities of the State policy of Ukraine. Strategic priorities. *Series: Politics, 3*(40), 65–67. https://acortar.link/AEx1pR

Telenyk, S. (2018). The Experience of Legal Regulation of the Critical Infrastructure Protection System in the United States. *Scientific Bulletin of the National Academy of Internal Affairs, 2*(107), 358-370. https://elar.naiau.kiev.ua/server/api/core/bitstreams/954b821f-edec-4d84-b3fa-845121cc79dc/content

The White House (1998). *Presidential Decision Directive/Nsc*-63. https://irp.fas.org/offdocs/pdd/pdd-63.htm

UNODC (2010). *The Globalization of Crime: a Transnational Organized Crime Threat Assessment*. Vienna: United Nations Office on Drugs and Crime. https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

Williams, P. (2001). Transnational criminal networks. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 61–98). RAND Corporation. http://www.jstor.org/stable/10.7249/mr1382osd.8

Yermenchuk O. (2018). *Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine*: monograph. Dnipro: Dnipropetrovsk state University of Internal Affairs. https://er.dduvs.edu.ua/handle/123456789/2371

Yermenchuk, O. (2017). The essence and content of the concept of "infrastructure" in the context of critical infrastructure protection. *Bulletin of the Ministry of Justice of Ukraine, 11*, 35-41. https://acortar.link/sorWuU

Yermoshenko, M., & Horiacheva, K. (2010). *Financial component of economic security: state and enterprise*: monograph. Kyiv: National Academy of Management. ISBN 978-966-8406-52-2