International Comparative Jurisprudence 2025 Volume 11 Issue 2
ISSN 2351-6674 (online) DOI: https://doi.org/10.13165/j.icj.2025.11.02.009



CORRUPTION AT THE CROSSROADS OF SECURITY: EXPOSING THREATS, BUILDING DEFENCE/RESILIENCE

Žaneta Navickienė[1]
Mykolas Romeris University, Lithuania
E mail: zaneta.navickiene@mruni.eu

Ilona Tamelė[2]
Mykolas Romeris University, Lithuania
E mail: ilonatam@mruni.eu

Mykhaylo Shepitko[3]
Yaroslav Mudriy National Law University, Ukraine
Email: shepitkomichael@gmail.com

Received: 1 October; accepted:21 November 2025.
DOI: https://doi.org/10.13165/j.icj.2025.11.02.009

Abstract. The paper discusses the importance of a systems approach in managing corruption threats to national security and highlights the potential of innovative approaches and technologies in mitigating these risks. The aim of this article is to show how corruption affects public and private sector actions, strategies and policies by examining the complex relationship between corruption and its impact on national security. To achieve this aim, the study focuses on identification corruption-related threats to national security, reviewing states' obligations to strengthen national security measures and assessing the experience of Lithuanian companies in identifying corruption risks in the field. The research combines a theoretical analysis of scientific literature with a quantitative method—a questionnaire survey conducted among Lithuanian state-owned and private companies. Based on the insights of scientists, it is estimated that certain national security interests may be violated by such illegal actions as weakening the institution, causing a dangerous increase in crime, unbalancing defence spending or damaging important infrastructure, increasing social and economic instability, etc. The results indicate that corruption risks related to national security must be managed systemically, through coordinated criminal, political, organisational and preventive measures, including personnel vetting, cybersecurity and procurement control. Innovative technologies such as artificial intelligence and blockchains can effectively reduce risks. The results obtained may serve as a starting point for Ukraine to strengthen the link between prevention of corruption and national security.

Keywords: National Security, Corruption, Threats, Corruption Resilience.

Introduction

Recent events such as the Russian war in Ukraine, tensions in other regions such as Israel, increased migratory flows and attempts to cross the US border, attempts by migrants from the Belarusian side to cross the borders of Lithuania, Latvia and Poland, and other unrest in the world all point to the need to revise the entire scale of the concept of security, from the perception of a sense of security and the notion of national security, to the development of reasonable and systematic responses to manage threats to national security. At the same time, these developments are also triggering research and evaluation in

[1]Professor of the Public Security Academy at Mykolas Romeris University. ORCID ID 0000-0002-8402-6333. Research interests: Criminalistics, Corruption Prevention, Organization of Pre-trial Investigation, Public Security.
[2] PhD student, Junior Assistant of the Public Security Academy at Mykolas Romeris University. ORCID ID 0000-0002-7019-7254. Research interests: Criminal Compliance, Criminal Corporate Liability, Criminalistics Techniques.
[3] Professor of the Criminal Law Department at Yaroslav Mudriy National Law University. ORCID ID 0000-0002-7164-8037. Research interests: Criminal Law, Criminal Liability, Crime against Justice, Criminalistics, Criminalistics Methods, Criminalistics Techniques, International Criminal Law.

this field, with the legitimate question of whether and how the nature of national security threats has changed and, if so, how they relate to other sectoral areas.

The Heritage Foundation in the Americas identifies several main groups of non-military national security: political security (protection of the government and the public from internal and external threats); economic security (control of the economy and people's freedom to control their own financial decisions); energy security (access to energy resources); homeland security (control of airports, borders, transport and migration); cyber security (Holmes, 2015).

Each sector's approach to security is determined by unique factors, which emphasises the importance of focusing national security strategies on vital areas and allocating resources efficiently (Holmes, 2015).

The multidimensional, ambiguous concept of security is a matter of debate in the scientific community (Pūraitė & Šilinskė, 2017). K.R. Holmes, in discussing what national security is and is not, stresses the need to clearly differentiate between national issues, emphasising the importance of focusing strategic planning on the vital aspects of national security, with a clear distinction between these and social and other domestic issues. He argues that this will help to avoid confusion and to allocate resources more efficiently, while ensuring real national defence (Holmes, 2015).

The fight against corruption is considered a national security priority. In regarding corruption as a threat to national security, Lithuania has included targeted provisions in the National Corruption Prevention Agenda, noting that "progress in combating corruption not only affects the maturity of society, the economy, state governance and the justice system, but also helps to ensure national security interests". The impact of corruption on national security is primarily visible through its effects on the functioning of state institutions. Corruption poses a threat to national security because it creates conditions for non-transparent activities of state institutions, undermines economic and social stability, fuels crime and erodes public trust in the state and its institutions (Seimas of the Republic of Lithuania, 2022, Section 1).

The various world events and unrest that destabilise the foundations of security in the scientific field make it possible to rethink the concept of national security, to assess the relationship between national security and civil society (Kazlauskaitė Markelienė & Petrauskaitė, 2011), and to evaluate what preventive measures are effective in ensuring national security.

Analysis by the U.S. Agency for International Development (USAID) has shown that in order to effectively address anti-corruption as a national security priority, there are three key areas that need to be the focus. Firstly, the development of flexible public procurement systems, e.g. The Office of Transition Initiatives (OTI) has developed procurement mechanisms that can be quickly adapted to different situations, making efficient use of people and resources. Secondly, the deployment of staff, e.g. in the field, in the form of "a pool" of staff. In addition, the Office of Humanitarian Aid deploys Disaster Assistance Response Teams (DARTs) that are ready to act quickly after a disaster. In addition, these teams could accordingly operate in anti-corruption situations, implementing the "corruption declaration" under clear conditions for rapid response. Thirdly, confidence building, e.g. USAID's violence and conflict prevention teams use confidence building techniques that can be adapted to anti-corruption initiatives to gain support from local communities and promote cooperation (Cordell, 2021).

Mr Cordell also stresses the importance of aligning political objectives with operational imperatives, of working with United Nations agencies on joint anti-corruption efforts and of participating in initiatives such as the G7 Build Back Better World (B3W) initiative, the aim of which is to fight corruption in infrastructure in a coherent manner. It also stresses the need to focus efforts on high-risk sectors such as green energy and digital technologies, to join and support initiatives such as the Extractive Industries Transparency Initiative (EITI), and to apply digital development principles to increase transparency and accountability (Cordell, 2021).

In examining security challenges, security aspirations and the avoidance of crises, conflicts, threats and hazards, scholars point to the need to address threat management in a systemic manner, i.e. "every crisis, conflict, threat or hazard must be understood and assessed in a systemic manner" (Melnikas et al., 2020, p. 401). Therefore, it is fully accepted that a systemic assessment is necessary since it is not focused on the analysis of individual phenomena and threats but on the correlation and impact of phenomena and processes on each other. It is thus agreed that the perception and assessment of threats and hazards as a system should be based both on the desire to clearly and unambiguously define the relevant boundaries of the system, and on the need to respond in a targeted, timely and effective manner to various crises, conflicts, threats, hazards and security problems (Melnikas et al., 2020, p. 403).

The analysis of scholarly sources shows that the impact of corruption threats on national security is defined more broadly, not only in terms of the impact on security or on individual security-related links, but also on human rights and the territorial integrity of the state. Scientists mentioned that "in Ukrainian society, corruption is a priority in the context of financial and military support" (Kravtsov et al., 2024, p. 28). Other authors, for example, O. Makarenkov, in his analysis of the impact of corruption threats on Ukraine's national security, notes that "the strategy of eliminating corruption threats to national security is a system of knowledge about legal and organisational measures aimed at ensuring the dominance of human virtues in public relations at a level that excludes both potential and real threats to human rights, territorial integrity, safe living conditions of citizens and other constitutional values" (Makarenkov, 2024, p. 173). It is important to note that a systemic approach to analysing national security challenges allows for a broader assessment of the scope of threats, i.e. to assess the parallels – what are the actions of other actors and how do they affect national security. Furthermore, at the same time, by looking at the scale of national security challenges in a systematic manner it is possible to identify not only national security risks in the narrow sense, but also the risks of other affected areas that impact national security. It should be noted that the timely and systematic identification of important risks allows for timely and adequate preparation for risk management (preparation of risk maps, identification of interrelated risks, development of risk management models, etc.). Researchers examining corruption risks have noted that "the main factors for the emergence of corruption in Ukraine are war, low standard of living, unfavourable crime situation, social stratification, distrust of the judicial system, isolation of power from society, weak anti-corruption legislation, migration" (Sobko et al., 2023, p. 223).

This article focuses on the main challenges of corruption in the field of national security, i.e. it will analyse how corruption can manifest itself in actions related to national security. This article seeks to show how the fight against corruption is inextricably linked to national security, and how the threat factors are strongly intertwined, requiring an integrated strategy and synergies and coherence between all actors.

The subject of this study is corruption risks in national security and their management.

The aim of this article is to show how corruption affects public and private sector actions, strategies and policies by examining the complex relationship between corruption and its impact on national security.

In order to achieve this objective, two objectives are set:
1) Identify corruption-related threats in the field of national security.
2) To review the obligations of states to strengthen national security measures and to assess the experience of Lithuanian companies in identifying corruption risks in the field of national security and in applying countermeasures.

The research used the method of analysis of scientific literature to analyse the theoretical provisions: definitions of corruption threats and national security; the impact of corruption threats on national security; the main insights of scholars regarding the relationship between national security and corruption. A quantitative research method—a questionnaire survey—was also used to analyse the experience of Lithuanian state-owned and private companies in identifying corruption threats and their impact on national security, as well as in applying countermeasures to manage such threats and ensure

national security. For this purpose, a questionnaire consisting of nine questions was administered to employees responsible for corruption prevention and/or national security (compliance officers) in these companies. The survey was conducted between August and September 2024, and the empirical findings are used in the article selectively, insofar as they directly relate to the issue under examination (Law on the Protection of Objects Important for National Security, 2002, Annex 1).

AI-assisted technology was not used in the preparation of this article.

1. Corruption threats in the context of national security

Different threats to national security caused by corruption can be identified, such as the weakening of democracy and trust in government, the strengthening of authoritarian regimes, the violation of state sovereignty, the fuelling of conflicts, the weakening of the state and its institutions and the growth of social discontent (Kukutschka, 2023). Corruption can also contribute to terrorism (Auer & Meierrieks, 2024) and migration threats, breaches of information and cyber security (Department of State Security of the Republic of Lithuania & Second Department of Operational Services, 2023, p. 54), economic instability and the vulnerability of strategic assets, thereby threatening public security. In addition, by weakening law enforcement and judicial institutions, corruption creates favourable conditions for organised crime to expand and operate with impunity and can be deliberately used by foreign states or non-state actors to buy influence through political and business networks, thereby deepening external interference in domestic decision-making (Khrystynchenko et al., 2023; Lang et al., 2025). Corruption may also distort defence spending (Ofori-Mensah & Zhelyazkova, 2024), diverting resources from the most urgent capability needs to less effective but more profitable projects for corrupt officials, and undermine the quality and resilience of critical infrastructure (such as roads, bridges and energy systems), creating additional vulnerabilities that can be exploited in crises or armed conflict. (Chen, Liu & Lee, 2022; OECD, 2022; Hawkins, 2013). In addition, links between corruption and national security are also important for future training. In the context of the long-term training of law enforcement officers for 2026–2029, it should be emphasised that due to changing phenomena and emerging prohibitions, such as the application of sanctions, it is necessary to share international good practices in investigating corruption-related crimes that are related to hybrid threats and sanctions circumvention; only in this way, will it be possible to build common security (Caciuloiu, 2025).

Scientists, in analysing corruption impact to social relations in Ukraine, stressed the necessity to continue applying a complex of anticorruption measures: “preventing and combatting corruption have been central to Ukraine’s reform agenda since the Revolution of Dignity in 2013-2014, and the increased transparency and preventive measures have led to tangible reductions in corruption across various sectors. However, corruption remains a major problem, causing significant costs to the state budget, businesses and the population, discouraging investment and undermining the rule of law by the Commission Opinion on Ukraine’s application for membership of the European Union, 2022” (Novikovas & Fedchyshyn, 2025, p. 91).

Recognising the seriousness of these threats and highlighting their interconnectedness requires a strong set of comprehensive measures, both nationally and internationally, to prevent corruption and to counter other threats. It must also be understood that anti-corruption strategies need to be flexible and dynamic, taking into account the ever-changing geopolitical situation and integrating with other national security strategies.

At the organisational level, a risk-based approach to tackling corruption, including clear anti-corruption policies, independent project evaluation, transparent decision-making criteria and the implementation of strong internal control systems, is crucial (Pattanayak & Verdugo Yepes, 2020). This is not only to reinforce the existing controls, but to also develop flexibility and the ability to act in uncertain situations, where innovation and experimentation are becoming essential. Mr. Lindstedt points out that 'antifragile' organisations are all about fostering a culture of experimentation within the organisation, empowering innovative teams and having leaders/managers who adapt their leadership style to lead appropriately in critical situations (Lindstedt, 2022).

Lithuania's national security assets, such as strategic companies and infrastructure, may expose it to the risk of corrupt practices, which could be reflected in the activities of these companies and put society at risk. If corruption becomes entrenched in strategic facilities, it can lead not only to economic losses but also to a direct threat to the security of the population and the stability of the state.

In order to identify corruption risks, the results of internal investigations and preventive analyses of Lithuanian companies and interviews with compliance officers of Lithuanian companies were used to identify actions that threaten national security and to assess their correlation with corruption resilience, cybersecurity and information security (see Figure 1).

Looking at the correlation in the context of national security, there are interlinkages between the individual areas of corruption resilience, cybersecurity and information security, and specific actions, where actions such as lack of cooperation, lack of regulation or fraudulent actions are linked to all areas in which national security can be affected.

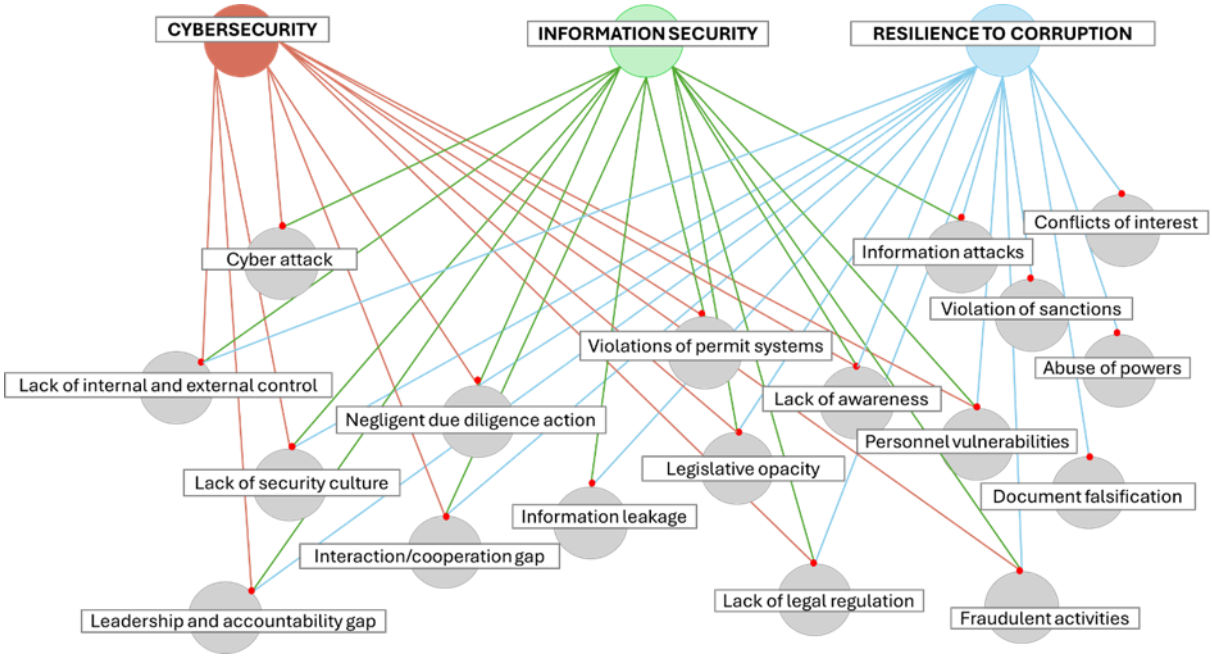


Figure 1. Correlation between threat-related actions and individual safety areas (prepared by the authors)

These actions can not only directly affect the operation of strategic facilities but also jeopardise the security of the country as a whole. However, they can be managed and mitigated through appropriate prevention and control measures and by integrating such measures into other national security strategies to ensure their effectiveness and coherence.

2. National security measures to enhance resilience to corruption: the Lithuanian experience

Each state needs to rethink its security model and adapt to changes both globally and regionally, which is also reflected in national legislation: the ability to operate in a less predictable environment, to cooperate more effectively with allies and partners, and to increase the resilience of the state and the public to emerging threats (Seimas of the Republic of Lithuania, 2021). Such actions are linked to measures of a complex nature in both internal and external contexts: deterrence, defence, building resilience to national security threats, and prevention of corruption. For example, the links between national security and the prevention of corruption are inseparable and are enshrined in key strategic documents, which stress that the anti-corruption system in Lithuania "cannot be static, but must be improved and developed in the light of changes, taking into account the link between corruption and national security: corruption should be seen as a threat to national security, and the fight against corruption is a prerequisite for and a key component of national security" (Seimas of the Republic of

Lithuania, 2022). Security requires states to take steps to identify security risks and to provide countermeasures to manage them.

More recently, legislation adopted by the European Parliament and the Council of the EU on a high common level of cybersecurity across the EU has entered into force. The aim is to further improve the resilience of the public and private sectors and the EU as a whole, as well as the resilience and incident response capabilities of the EU. This is in order to harmonise the cybersecurity measures taken by the Member States, to lay down the key rules for the operation of a coordinated regulatory framework and to establish mechanisms for effective cooperation amongst the authorities responsible in each Member State (European Parliament & Council, 2022). Compliance with these provisions would not only ensure the management of risks related to information security, e.g. by defining the responsibilities of the responsible actors in the field of information security, but also manage potential corruption risks, e.g. to prevent the possible leakage of confidential information.

The General Data Protection Regulation and other legislation on personal data protection require you to take steps to ensure the protection of personal data in order to prevent personal data breaches. In this context, it is important to assess the appropriateness of the transfer of data to third parties in order to foresee that the data will be used for a specific purpose (drafting of data transfer agreements). At the same time, however, it is important to identify and justify the nature and content of the anti-corruption measures to be implemented, the content of the targeted data, and the need for publicity in the public interest (General Data Protection Regulation, 2016).

The unauthorised loss, destruction, disclosure or unauthorised access to, or disruption of, an information system, technology or computer equipment of companies and organisations is an act that can affect the performance of companies and organisations and cause them material or non-material damage. Therefore, States are obliged to develop and implement cyber security incident and vulnerability (security gap) management plans to establish procedures for companies and organisations to properly manage cyber and information security incidents and cyber vulnerabilities identified in companies and organisations information systems, technologies, computer equipment and electronic communications networks (General Data Protection Regulation, 2016).

In addition, each country takes other steps to ensure national security and other security links. Lithuania, for example, has clarified the link between national security and anti-corruption activities (Seimas of the Republic of Lithuania, 2022). The National Anti-Corruption Agenda 2022-2033 states that “the objective of preventing corruption is to strengthen national security, create social welfare, improve the quality of administrative, public and other public services, protect freedom of fair competition, and minimise the impediment of corruption to the development of democracy and the economy” (Seimas of the Republic of Lithuania, 2022). Corrupt acts are understood more broadly to include acts aimed at concealing corruption offences, while the implementation of corruption-proof measures requires an assessment of the relationship between corruption prevention and national security, etc.

Secondly, Lithuania obliges companies of national security importance to prepare Security Plans (Seimas of the Republic of Lithuania, (2024b), Art. 15), which provide for the application of information security, cyber security, personnel security and physical security measures to manage potential risks in the companies' areas of activity. Recently, new challenges have been raised in relation to these plans, such as the activation of the plans when needed and the evaluation of the effectiveness of their provisions by means of exercises to determine whether the provisions of the security plans are effective in ensuring the security of the companies' operations. Other undertakings and organisations that do not qualify as undertakings of national security importance should, among other things, prepare security plans in accordance with the nature and specificity of their activities and apply basic regulatory measures, such as confidentiality undertakings, to their operations.

Thirdly, in Lithuania, companies of national security importance, in accordance with targeted legislation (Seimas of the Republic of Lithuania, (2024b)), must assess their compliance with national security requirements by applying to a special commission before entering into transactions. In addition, investor

due diligence is compulsory in the cases set out in the aforementioned law. In all cases, it is necessary to identify the risks arising in the field of national security and to provide measures to manage them.
Fourthly, Lithuania needs to fulfil the eligibility requirements for persons applying for or holding positions in companies important for national security. Ensuring compliance is linked to the management of potential risks in the field of national security through the selection and recruitment of reliable and transparent personnel. The correlation of compliance is seen in the area of personnel reliability: not only under Article 17 of the Law on the Protection of Objects of National Security Importance, but also under Article 17 of the Law on the Prevention of Corruption. In a complex assessment of the relationship between national security and corruption prevention, an analysis of the legal basis and application of these security checks reveals not only the close parallelism between the procedure of the checks, but also between the objectives themselves, (Navickienė & Kinkevičius, 2023).

It should be noted that additional cross-cutting actions have recently been taken to ensure national security. The changing geopolitical situation has led to a review and tightening of national security procurement requirements (Seimas of the Republic of Lithuania, (2024a, 2024c)). The relevant legislation has been substantially supplemented with national security provisions, which include the need to ensure that the entity has no interests that could jeopardise national security, the origin of the goods to be procured etc.

The authors' research has shown that depending on the nature of their activities, companies and organisations are implementing and enforcing other effective national security, information security, cybersecurity and anti-corruption measures that comprehensively address national security interests, but companies are not doing it to a great enough extent.

The survey covered one public institution, one state-owned enterprise, ten state-owned joint-stock companies (closed joint-stock companies), one municipally owned joint-stock company and one foreign-owned private company (Figure 2). The low participation of private companies is explained by the fact that only a few state-owned and private companies were selected from the list of companies of national security importance on (Law on the Protection of Objects Important for National Security, 2002, Annexes 1–3) in order to get an overall picture of the representation of these sectors and their importance for national security.

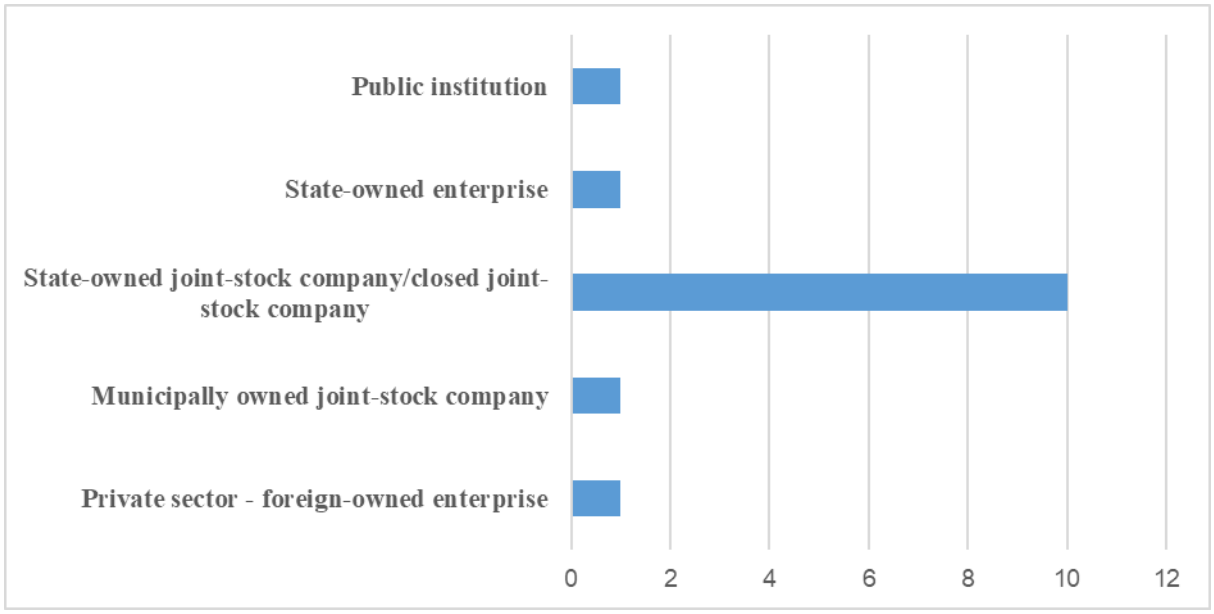


Figure 2. Company forms

Thus, the survey data suggest that state-owned joint-stock companies/ closed joint-stock companies are the most exposed to various risks, in particular information leakage, cyber-attacks, disclosure of commercial or official secrets, evasion of sanctions and other violations of sanctions, and non-performance of official duties.

State-owned enterprises and municipally owned joint-stock companies are also exposed to certain risks, with a lower risk distribution than state-owned companies, but are still exposed to cyber-attacks and other criminal activities.

The private sector has a lower diversity of risks compared to public enterprises and companies, but is exposed to risks of theft, fraud and bribery and kickbacks.

In summary, cyber-attacks and information leaks are the most common risks in all categories analysed, especially in state-owned joint-stock companies/ closed joint-stock companies. These risks in state-owned joint-stock companies/ closed joint-stock companies are particularly frequent. This may reflect their greater importance, sensitivity or attraction to malicious actors seeking to obtain sensitive information or disrupt operations (Figure 3).

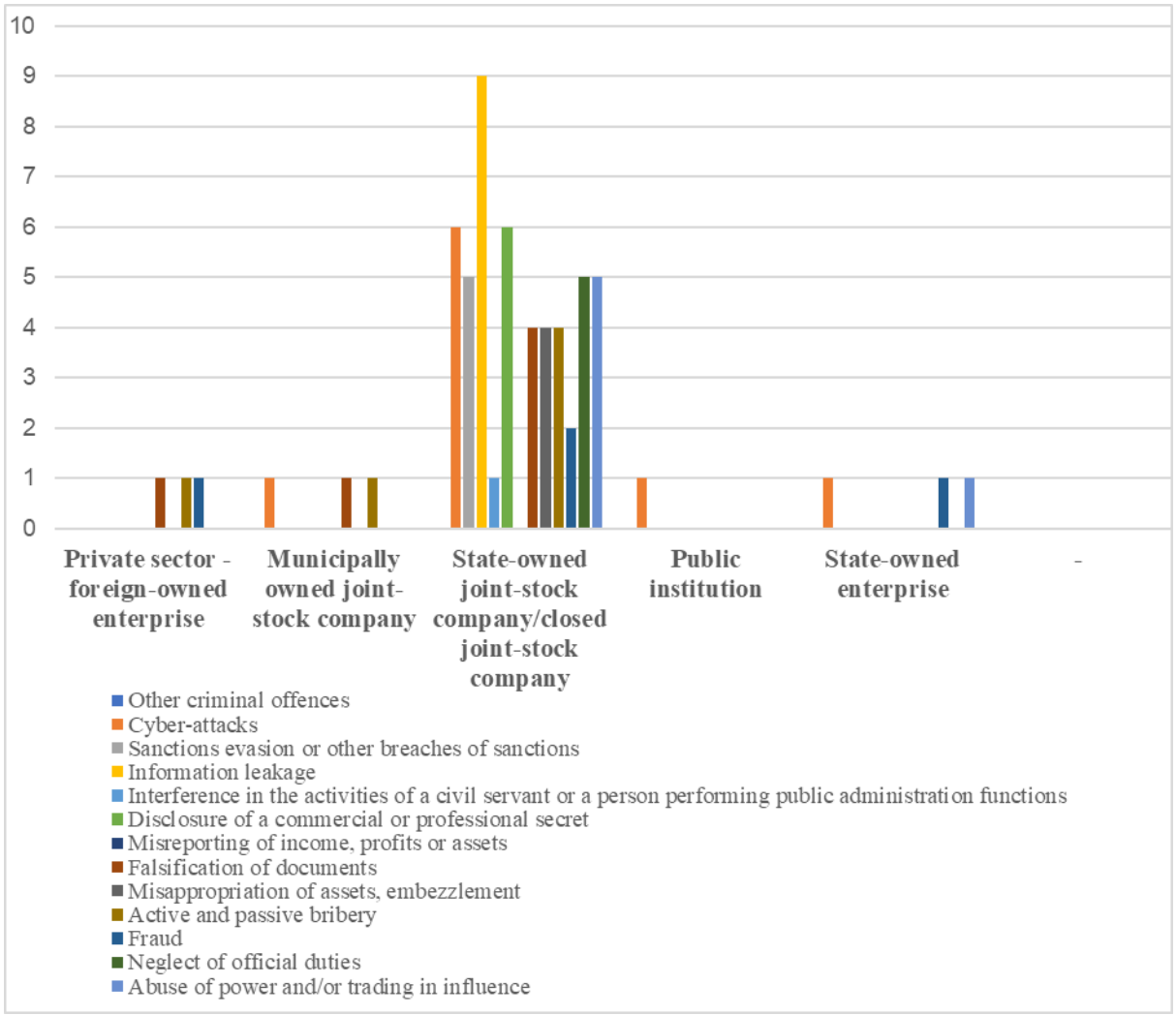


Figure 3. Which types of corruption and other criminal offences pose the greatest threat to your company's national security interests?

The initial findings of the survey suggest that organisations value most the implementation of comprehensive internal policies and procedures (12 responses), as well as the establishment of dedicated anti-corruption units (9 responses) and internal and external audits (9 responses) (Figure 4).

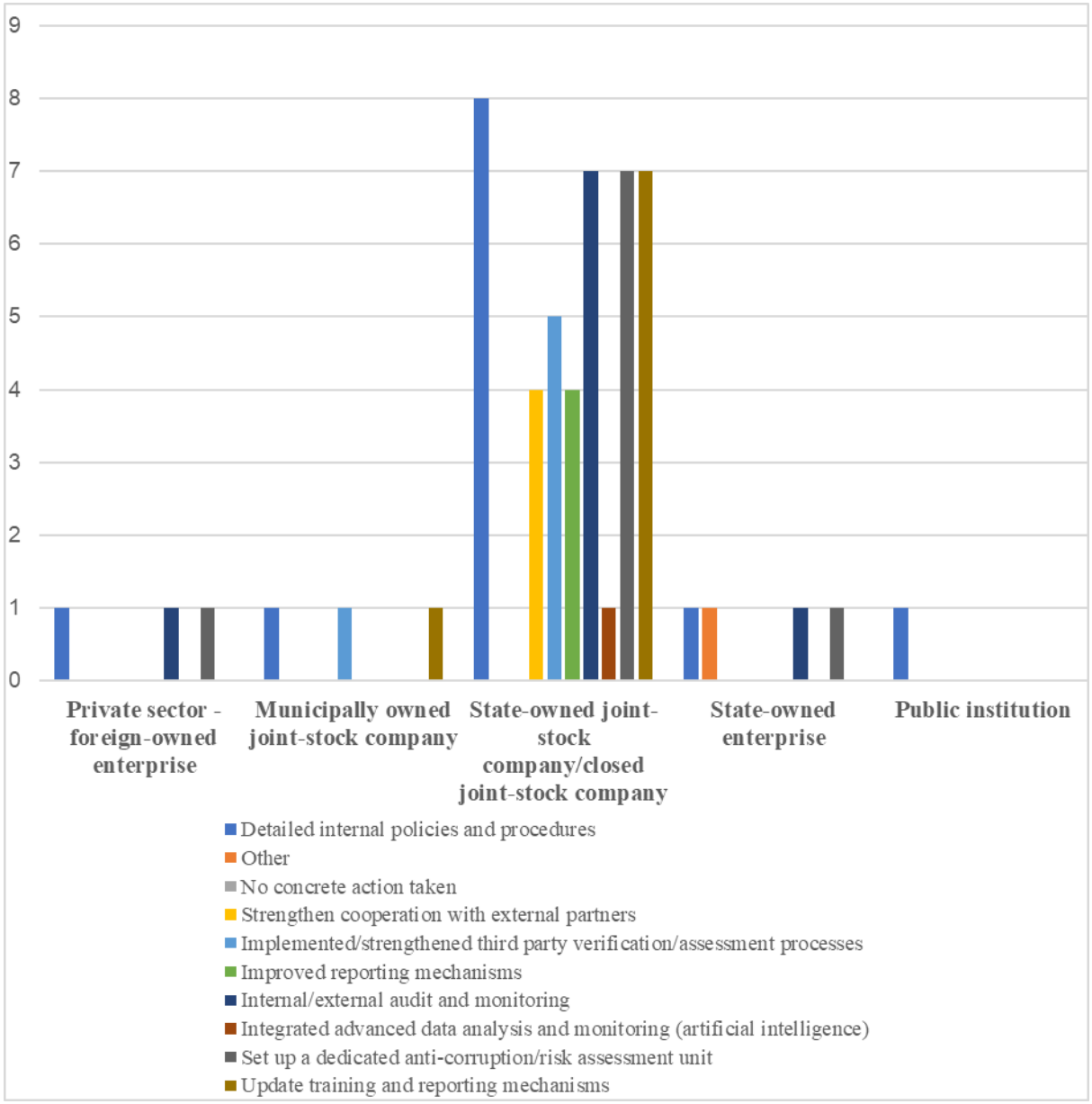


Figure 4. What steps has your company taken to identify and respond to these new threats?

In addition, state-owned joint-stock companies/ closed joint-stock companies are active in implementing other measures to identify and respond to new threats. They often strengthen cooperation with external partners, introduce third party verification processes and improve reporting mechanisms. In contrast, some private and municipally owned companies are less active in these areas, which may reflect different priorities and principles. These differences may be due to different legal frameworks for risk management and compliance and the availability of resources. Private companies may manage risks differently as they often face fewer bureaucratic hurdles and have greater flexibility. The private sector can focus on targeted risk management and need only act when necessary, thus avoiding excessive costs and making more efficient use of resources.

Therefore, while state-owned joint-stock companies/ closed joint-stock companies use a variety of measures, this does not necessarily show the superiority of their methods. Private companies may operate in a different way, concentrating on key areas and making the best use of available resources.

In assessing the effectiveness of measures, it is necessary to consider the specific context and characteristics of the companies' activities and to carry out appropriate further research.

The tools in place help to identify threats, ensure legal compliance and transparency in organisations. However, when discussing other measures that can improve the effectiveness of the fight against corruption in national security companies, the survey data shows that state-owned joint-stock companies/ closed joint-stock companies highlighted the need to invest more in training and awareness-raising of employees, clear regulation of processes and technology-based monitoring.

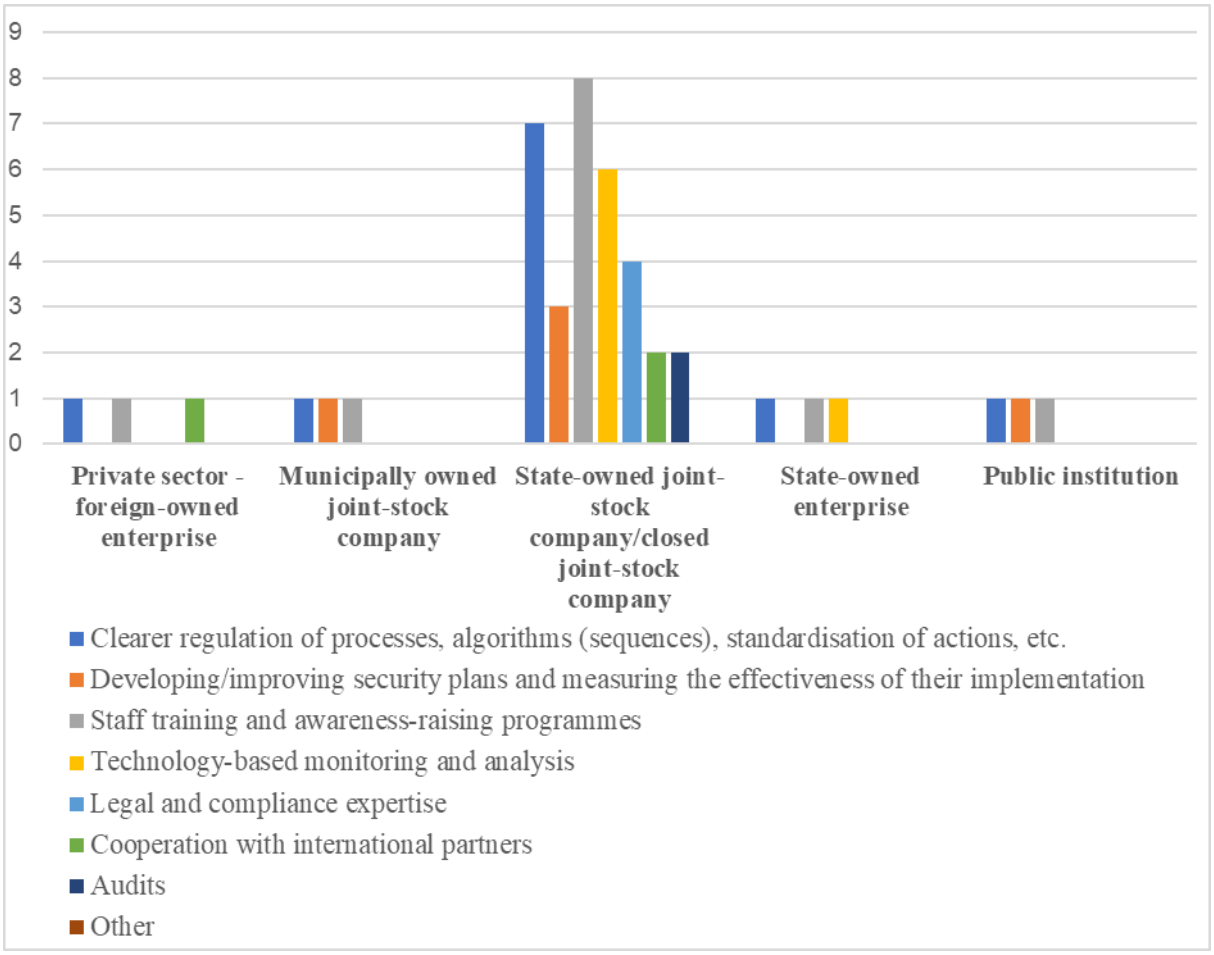


Figure 5. Are there any specific areas where national security companies should invest more to improve their anti-corruption efforts?

When analysing which innovative approaches or technologies can effectively reduce corruption and other related risks (Figure 6), several trends can be observed. state-owned joint-stock companies/ closed joint-stock companies consider that being more proactive in using different technologies and methods is an effective way to fight corruption. Compared to other forms of organisations, they particularly value artificial intelligence technologies for data analysis and anomaly detection, and blockchain technology for transparent supply chains. This approach may be linked to a greater need for transparency and strict compliance requirements, at least from a regulatory perspective. The use of risk maps is also seen as important in both state-owned joint-stock companies/ closed joint-stock companies and the private sector. Furthermore, private companies consider the introduction of advanced technologies such as digital whistleblower platforms as an effective way to reduce corruption. Different technologies are valued in different organisations, depending on their specific needs and field of activity, but there is a trend where advanced technologies are becoming an increasingly important tool in the fight against corruption and in the strengthening of organisations' security systems.

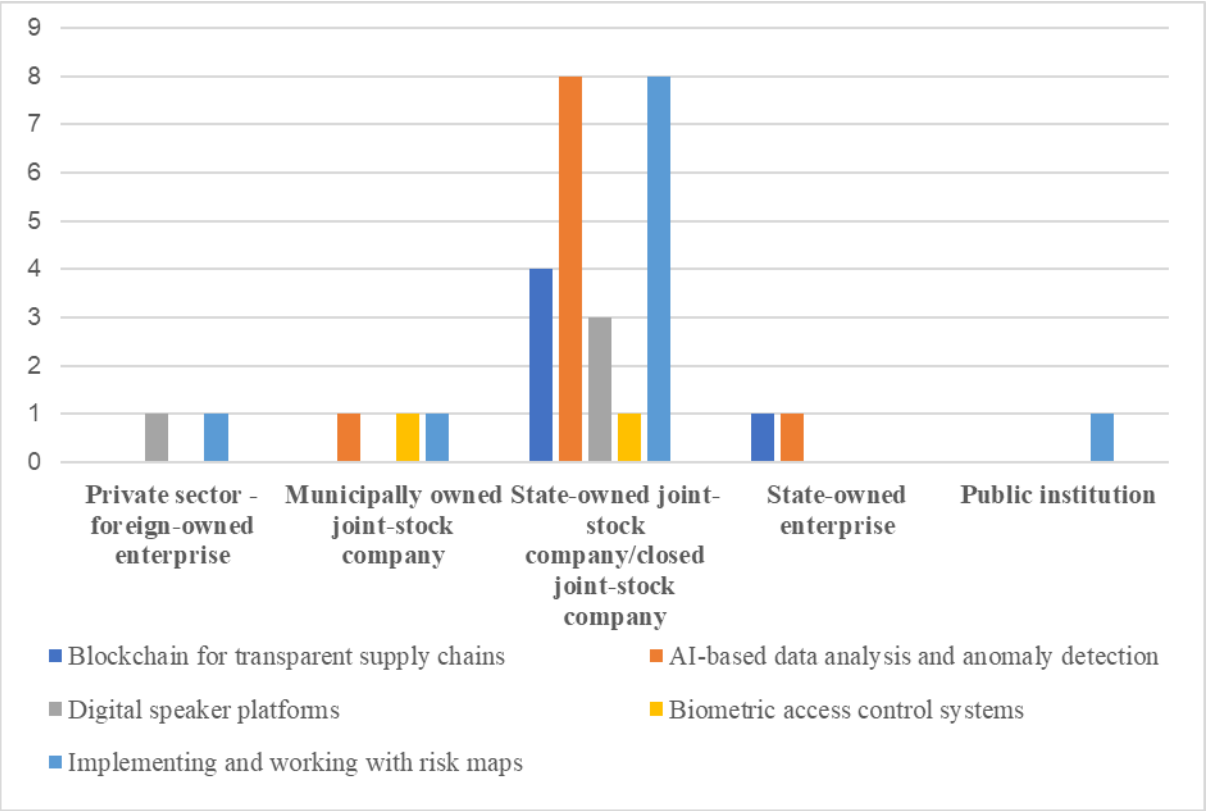


Figure 6. Which innovative methods or technologies do you think can effectively reduce corruption and other related risks?

In summary, Lithuanian companies are confronted with corruption in national security. They recognise such threats and apply different countermeasures; in particular, state-owned joint-stock companies/ closed joint-stock companies have paid a lot of attention to strengthening the targeted provisions of their internal legislation, to strengthening third-party verification, and to audits and monitoring. However, at the same time, they are concerned about the need for more active awareness-raising, clearer regulation of the processes, better integration of technologies for monitoring, and innovative ways and actions to reduce corruption.

After evaluating the experience of Lithuanian companies, comparing and transforming (modelling) the results obtained, the following experience would be significant for Ukraine in the field of strengthening national security. Criminal policy in the field of national security has several vectors: 1) countering war challenges; 2) countering corruption challenges; 3) preserving the Euro-integration and Euro-Atlantic directions of Ukraine's development. At the same time, national security itself in the modern world consists of many components: cybersecurity, information security, environmental security, etc. That is why Lithuania's experience in the fight against corruption is important, especially taking into account the creation of a reliable legislative framework, effective anti-corruption law enforcement and judicial bodies, and the creation of mechanisms for their interaction at the EU level. In addition, Lithuania, as an EU member state, has gone through the procedure of adapting its legislation to EU legislation (in accordance with agreements, regulations, directives, etc.), which provides an opportunity to form a criminal policy in the field of national security of Ukraine considering the experience of Lithuania. The empirical data obtained allow for Ukraine to identify corruption risks during the future transition from EU candidate state to the full EU member state.

Conclusions

Corruption is one of the biggest threats to national security, with a wide-ranging impact on both the state and society. In the context of national security, corruption takes many forms, including leaks of confidential information, sanctions violations, lack of awareness, cyber-attacks, etc. The fight against corruption requires comprehensive, flexible and dynamic strategies integrated into national security plans. They must promote transparency, strengthen control and ensure long-term stability. The systemic approach includes not only criminal prosecution but also political, organisational and preventive actions (personnel vetting, cyber-security, procurement control). Innovative technologies such as artificial intelligence and blockchains can effectively reduce risks.

The study shows that state-owned joint-stock companies/ closed joint-stock companies are more exposed to corruption risks than private companies. They are quite active in implementing measures to identify and respond to new threats, but there is still a greater need to strengthen legal compliance management systems, deploy advanced technologies, model potential threat scenarios and strengthen corporate preparedness for practical action.

Based on the results obtained, Ukraine could beneficially adopt Lithuania's best practices in anti-corruption policy and the development of national security-oriented criminal policy.

References:

Auer, D., & Meierrieks, D. (2024). Bestechung und Bomben: Korruptionsbekämpfung dient auch der nationalen Sicherheit. *WZB-Mitteilungen: Quartalsheft für Sozialforschung*, (186), 48–50. https://bibliothek.wzb.eu/artikel/2024/f-26651.pdf

Caciuloiu, A. (2025, November 14). Challenges and opportunities for officer training in creating a common EU law enforcement culture. Presentation at the international conference *Police in a changing world*, Seimas of the Republic of Lithuania, Vilnius.

Chen, C., Liu, C., & Lee, J. (2022). Corruption and the quality of transportation infrastructure: Evidence from the US states. *International Review of Administrative Sciences*, 88(2), 552–569. https://doi.org/10.1177/0020852320953184

Cordell, K. (2021). Anti-corruption as a national security priority: Planning the development response. Center for Strategic and International Studies. https://www.csis.org/analysis/anti-corruption-national-security-priority-planning-development-response

Department of State Security of the Republic of Lithuania, & Second Department of Operational Services under the Ministry of National Defence. (2023). *Assessment of threats to national security 2023*.

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union*, L 119, 4.5.2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). *Official Journal of the European Union*, L 333, 27.12.2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Hawkins, J. (2013). How to note: Reducing corruption in infrastructure sectors. *Evidence on Demand*. https://doi.org/10.12774/eod_cr.may2013.hawkins

Holmes, K. R. (2015). What is national security? In *2015 Index of U.S. Military Strength*. The Heritage Foundation, Washington, DC.

Kazlauskaitė-Markelienė, R., & Petrauskaitė, A. (2011). Civil society and national security: A theoretical review of the problem. *Annual Strategic Review of Lithuania*, 9(1), 235–253.

Khrystynchenko, N., Tataryn, N., Hrokholskyi, V., Tomliak, T., & Starostin, O. (2023). Corruption in the civil service as a threat to national security. *Lex Humana*, 15(4), 414–426. https://seer.ucp.br/seer/index.php/LexHumana/article/view/2808

Kravtsov, S., Orobets, K., Shyshpanova, N., Vovchenko, O., & Berezovska-Chmil, O. (2024). Progress and challenges in combating corruption in Ukraine: Pathways forward. *Journal of Strategic Security*, 17(2), 28–43.

Kukutschka, R. M. B. (2023, January 31). CPI 2022: Corruption as a fundamental threat to peace and security. Transparency International. CPI 2022: Corruption as a fundamental threat to… - Transparency.org

Lang, B., Pozsgai Alvarez, J., & Hogic, N. (2025). Strategic corruption: Conceptualizing the geostrategic dimensions of transnational corruption. *Public Integrity*, 1–9. Advance online publication. https://doi.org/10.1080/10999922.2025.2520704

Lindstedt, D. (2022). *Building resilient organizations through change, chance, and complexity*. Taylor & Francis.

Makarenkov, O. (2024). Strategy for eliminating corruption threats to Ukraine's national security. *Baltic Journal of Economic Studies*, 10(1), 163–174.

Melnikas, B., Tumalavičius, V., Šakočius, A., Bileišis, M., Ungurytė-Ragauskienė, S., Giedraitytė, V., Prakapienė, D., Guščinskienė, J., Čiburienė, J., Dubauskas, G., Dudzevičiūtė, G. (2020). *Security challenges: Improving management.* Collective monograph. Vilnius: Ministry of National Defence of the Republic of Lithuania.

Navickienė, Ž., & Kinkevičius, A. (2023). Improving personnel security clearance – the way of harmonization of national and European Union legal acts. *Jurisprudence*, 30(1), 100–120.

Novikovas, A., & Fedchyshyn, S. (2025). Peculiarities of the legal regulation of accepting gifts in the civil service in Ukraine and Lithuania. *International Comparative Jurisprudence*, 11(1), 91–103.

OECD. (2022). *Catalysing collective action to combat corruption in infrastructure: Accountable and effective non-judicial grievance mechanisms*. OECD Publishing. https://doi.org/10.1787/ce6d1b84-en

Ofori-Mensah, M., & Zhelyazkova, D. (2024). *Trojan horse tactics: Unmasking the imperative for transparency in military spending*. Transparency International Defence & Security.

Pattanayak, S., & Verdugo-Yepes, C. (2020). Protecting public infrastructure from vulnerabilities to corruption: A risk-based approach. In *Well Spent: How Strong Infrastructure Governance Can End Waste in Public Investment*. International Monetary Fund.

Pūraitė, A., & Šilinskė, N. (2017). Understanding the concept of security: Theoretical approach. *Public Security and Public Order*, 19, 135–145.

Seimas of the Republic of Lithuania. (2021). *National Security Strategy* (Resolution No. IX-907 of 28 May 2002; current version as of 22 December 2021). Vilnius.

Seimas of the Republic of Lithuania. (2022). *National Agenda for the Prevention of Corruption 2022–2033* (Resolution No. XIV-1178 of 28 June 2022; TAR, 2022-07-07, No. 14816). Vilnius.

Seimas of the Republic of Lithuania. (2024a). *Law No. I-1491 on Public Procurement* (adopted 13 August 1996; Vilnius.

Seimas of the Republic of Lithuania. (2024b). *Law No. IX-1132 on the Protection of Objects Important for National Security* (adopted 10 October 2002; *Valstybės žinios*, 2002-10-30, No. 103-4604; current consolidated version as of 1 January 2024). Vilnius.

Seimas of the Republic of Lithuania. (2024c). *Law No. XIII-328 on Procurement by Contracting Entities in the Fields of Water Management, Energy, Transport and Postal Services* (adopted 2 May 2017; current consolidated version as of 1 May 2024). Vilnius.

Sobko, G., Shchyrska, V., Volodina, O., Kurman, O., & Semenohov, V. (2023). International anti-corruption concepts and their implementation in Ukraine. *Novum Jus*, 17(2), 219–249.

Copyright © 2025 by the author(s) and Mykolas Romeris University
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access