NUOVA ANTOLOGIA MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

# NAM Studies & Documents

## Special Dossier October 2025
## **Ukraine Military and Wartime Law**

Edited by Ganna Sobko

*Società Italiana di Storia Militare*

*Nuova Antologia Militare*

Rivista interdisciplinare della Società Italiana di Storia Militare

Periodico telematico open-access annuale (www.nam-sism.org)

Registrazione del Tribunale Ordinario di Roma n. 06 del 30 Gennaio 2020

Scopus List of Accepted Titles October 2022 (No. 597)

Rivista scientifica ANVUR (5/9/2023) Area 11, Area 10 (21/12/2024)

Direzione, Via Bosco degli Arvali 24, 00148 Roma

Contatti: direzione@nam-sigm.org ; virgilio.ilari@gmail.com



Grafica: Nadir Media Srl - Via Giuseppe Veronese, 22 - 00146 Roma

info@nadirmedia.it

Gruppo Editoriale Tab Srl -Viale Manzoni 24/c - 00185 Roma

www.tabedizioni.it

ISSN: 2704-9795

ISBN Fascicolo 979-12-5669-221-7

NUOVA ANTOLOGIA MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

# NAM Studies & Documents

## Special Dossier October 2025
## **Ukraine Military and Wartime Law**

Edited by Ganna Sobko


*Società Italiana di Storia Militare*


Monument to Yaroslav The Wise, Grand Prince of Kyiv (978-1054)
In the Yaroslav Mudryi National Law University,
61024, 77, Hryhorii Skovorody Street, Kharkiv, Ukraine
Photo Tala Tamila (2015) CC SA 4.0 (Wikimedia Commons)

# Intellectualization of financial investigations
## in the system of anti-corruption compliance of procurement in accordance with NATO standards in ensuring the stability of national security

by Karina Nazarova[1], Volodymyr Hordopolov[2], Tetiana Lositska[3]

Abstract. During warfare and martial law, Ukraine's defense procurement system requires urgent reform to ensure national security and effective international cooperation. Therefore, the study aims to propose practical steps for implementing NATO-aligned anti-corruption and investigative mechanisms in Ukraine's defense procurement, thus ensuring stability and security under martial law. The research applies methods such as analysis, synthesis, induction, deduction, dialectics, analogy, abstraction, and generalization to assess how intellectualized investigations and digitalization can mitigate corruption risks. As a result, it is established that the existing system fails to address high corruption risks and global market shifts, resulting in operational delays, inefficiencies, and diminished trust from international partners. Core issues include the duplication of powers, poor inter-agency coordination, and a lack of effective oversight, with corruption remaining the most critical threat. This study highlights the potential of intellectualized financial investigations and digital anti-corruption tools, aligned with NATO compliance standards, to strengthen control mechanisms and minimize human error. The NATO approach demonstrates that procedural flexibility and transparency are compatible, offering a viable model for Ukraine. The integration of advanced analytics, digital monitoring systems, and compliance protocols is essential for increasing transparency, enhancing procurement ethics, and reinforcing the country's Euro-Atlantic integration efforts.

Keywords: national security; corruption; NATO standards; public procurement monitoring; digitalization.

1 Doctor of Economics, Professor, Department of Financial Analysis and Audit, State University of Trade and Economics, 02156, 19 Kyoto Str., Kyiv, Ukraine. https://orcid.org/0000-0002-5019-9244.

2 Doctor of Economics, Professor, Department of Financial Analysis and Audit, State University of Trade and Economics, 02156, 19 Kyoto Str., Kyiv, Ukraine. https://orcid.org/0000-0002-3151-8035.

3 PhD in Economics, Senior Researcher, Research Department, State University of Trade and Economics, 02156, 19 Kyoto Str., Kyiv, Ukraine. https://orcid.org/0000-0003-3117-3281. t.lositska@knute.edu.ua.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922175
Ottobre 2025

*Introduction*

The full-scale armed aggression of the Russian Federation has created a significant burden on the defense procurement system of Ukraine, which further necessitated adaptation to new difficulties. In addition, it works during martial law, when the reliability and timeliness of supplies are critical needs. However, existing methods of organizing, planning, and conducting procurement do not take into account several modern problems, such as the high danger of corruption, the requirement to maintain efficiency and secrecy, as well as constant changes in the global market for military goods. This leads to irrational use of resources, delays in supplies, and a decrease in the confidence of foreign partners.

The defense industry is vulnerable to corruption schemes due to improper implementation of procurement policy by the Ministry of Defense of Ukraine, duplication of departmental powers, poor coordination, inadequate legal regulation, and ineffective control. According to Transparency International and the National Agency for the Prevention of Corruption (NACP), despite some improvements, corruption remains the main obstacle to the effective operation of the defense procurement system (Transparency International, 2024). This demonstrates that risk management practices urgently need to be thoroughly reformed and effective accountability and transparency systems introduced.

Digitalization of defense procurement procedures is one of the most potential areas for combating corruption risks. With the help of modern IT solutions, electronic platforms, digital registries, and analytical tools, it is possible to significantly reduce the influence of the human factor, increase control efficiency, guarantee procurement tracking, and quickly eliminate violations. At the same time, digital transformation should be included in a broader system of anti-corruption compliance by NATO standards, which include professional training of personnel, independent monitoring, as well as less freedom of action and responsibility.

The system can be improved by adapting best practices from around the world, especially the anti-corruption programs of NATO member states. This allows you to optimize costs and increase transparency while maintaining important procedural flexibility. By implementing such measures in practice, Ukraine will be able to increase its defense capability, form a favorable image abroad, and attract sponsors and partners.

This study identified important shortcomings in the current system, examined the relationship between the degree of digitalization of defense procurement and the reduction of corruption risks, and provided useful suggestions for the gradual implementation of anti-corruption compliance tools by world standards. In the context of further Euro-Atlantic integration of Ukraine, the full implementation of these technologies has the potential for a revolution in the country's defense procurement system, which will become modern, open, transparent, and honest.

Several scientists have investigated this direction of social relations in particular Pakhachuk et al. (2025) analyzed the experience of NATO, the USA, and the EU in managing the risks of defense procurement and suggested ways to adapt it in Ukraine. Emphasis is placed on digitalization, risk registries, staff training, and increased auditing to increase transparency and compliance with NATO standards. Shkola and Bakin (2024) studied the EU mechanisms for countering modern challenges and threats and outlined the possibilities of their adaptation to strengthen the security and stability of Ukraine. Rusina (2025) investigated the peculiarities of state financial control under martial law, identified key problems of its implementation, and proposed ways to increase efficiency to strengthen financial discipline and national security. Zhuravel (2024) examined the specifics of managing public finances in wartime conditions, identified problems of efficiency and accountability, and proposed ways to solve them to ensure the stability of public finances. Petrunyak (2023) analyzed the legal mechanisms for combating corruption in the financial sector, identified its vulnerability to corruption risks, and emphasized the need to improve legislation, financial control, and international cooperation, especially under martial law.

The aim of the study is to assess how digitalization can reduce corruption risks in Ukraine's defense procurement, to consider NATO anti-corruption standards and financial investigation procedures for the defense industry, and to create effective proposals for the implementation of these strategies in the country's defense procurement system, taking into account the requirements of Euro-Atlantic integration and the conditions of martial law.

## *Methodological Framework*

The approach in this study, which combines traditional general scientific and cognitive methodologies, allowed us to identify in detail corruption vulnerabili-

ties in the defense procurement system of Ukraine and offer practical solutions. The components of the defense procurement system were investigated through analysis in stages, from institutional structure and regulatory control to specific abuse situations. For example, the analysis investigated the situation with the "egg scandal" of 2023 - the actions of officials, the content of the contract, the validity of prices, and the availability of control were separately considered.

Synthesis was used to create a common risk management model that includes digital technologies, compliance initiatives, and anti-corruption audits. The proposal to combine the tasks of risk management, digitalization, and transparency into a single procurement policy architecture was made possible by synthesis. Induction was demonstrated by the development of broad generalizations to study specific cases, such as the acquisition of protective vests, the provision of material goods, and the inefficient use of the Food Catalog. General characteristics of corruption risks were derived based on system defects in each scenario.

Based on NATO's broad risk management guidelines, namely the ARAMP-1 standard, deduction has allowed us to confirm whether Ukrainian processes meet these standards. For example, a critical assessment of Ukrainian procedures for proper verification of contracts was carried out in the light of instructions to maintain risk registers. The study of the dynamics and contradictions of the procurement system - the need for rapid delivery during the war, on the one hand, and the requirements of transparency and control - on the other, became possible thanks to dialectical technology. This allowed us to identify the main conflict between the fight against corruption and procedural flexibility, which became the focus of the study.

The study of world experience (NATO, USA, EU) used analytical techniques; In particular, DFARS standards, Directive 2009/81/EC, and ARAMP-1 were taken into account. To find out if they can be adapted in Ukraine, a thorough analysis of relevant digital platforms such as PIEE in the USA and EBAU in Germany was conducted. Comparison of Ukrainian institutions with relevant organizations in NATO countries became possible thanks to the methodology of analogy. The idea of creating an independent audit unit is based on similar procedures in other jurisdictions, such as the State Audit Service, which is considered a possible analog of DCAA in the United States.

Key ideas and categories such as procurement system, corruption risk, digita-

lization, and compliance were defined through abstraction. As a result, we were able to exclude minor components and focus research on important risk factors. The research process ended with a generalization; Based on the collected facts, studied cases and comparison of world experience, system proposals for the digital transformation of defense procurement and the implementation of anti-corruption compliance have been developed. Using these methods, we were able to guarantee the breadth, consistency, and scientific validity of the research results, which allowed us to propose the proposed strategies as a basis for restructuring the defense industry of Ukraine.

## *Results*

The Ukrainian defense procurement system operates under conditions of extreme regulatory complexity and significant legal uncertainty during martial law, which increases the likelihood of systemic corruption. The presence of a large number of normative legal acts, such as laws, decrees of the Cabinet of Ministers, internal orders, and other documents, as well as frequent changes to them, complicate the understanding of procurement procedures, reduce the transparency and predictability of the process, create opportunities for abuse of power. In practice, special regulations, such as Cabinet of Ministers Resolutions No. 1275 or No. 1178, which specifically allow procurement without the application of legally established competitive procedures, often replace or repeal the Law of Ukraine "On Defense Procurement", even though it was created to regulate the basic principles of planning, conducting and controlling procurement for security and defense needs. Such exceptions may be acceptable as a short-term solution during a conflict, but their extended application favors corruption because it does not provide adequate accountability, control, and competition.

Of particular concern is the combination of the Ministry of Defense's responsibilities to develop and implement procurement policies, as they are contrary to good governance. This means that the same bodies or structural units are responsible for planning, contracting, determining needs, quality assurance, negotiating, and supervising the terms of the contract. This concentration of power leads to conflicts of interest and excessive discretion, which is especially risky when procurement processes are simplified or non-competitive. This has already resulted in certain corruption abuses, especially the purchase of low-quality body armor

for exorbitant funds, which cost the state more than a billion hryvnias. Law enforcement investigations confirm that DOD officials abused their authority by signing contracts with questionable suppliers through procedural loopholes, violating quality standards, and failing to properly verify counterparty qualifications (Zaremba & Lusta, 2021).

Duplication of efforts, belated decision-making, and reduced efficiency during the war is caused by the unclear role of ministries, in particular the Ministry of Defense, the Ministry of Economy, and the Ministry of Strategic Industry, which are involved in the planning and execution of procurement. Effective procurement planning, rapid response to the first requirements, and a high level of integrity and accountability are hampered by the lack of a single coordination structure, a clearly defined organization responsible for defense procurement policy, and a system of interdepartmental communication. The unification of the legislative framework, the creation of a single procurement body, the definition of clear powers, and the introduction of a long-term planning system based on the needs and life cycle of products are among the recommendations developed in cooperation with NATO experts as part of the Strategic Review of Defense Procurement.

In addition, procurement planning in logistics is often based on incomplete or delayed data and is carried out without proper analytics, especially when it comes to tangible assets. The lack of a clear time frame and method for harmonizing technical specifications with state-owned enterprises, such as DOT, leads to poor planning, delays, and cases where purchases are made as urgent without sufficient explanation. This allows you to choose non-competitive methods and contributes to an environment in which suppliers are identified non-transparently. The issue is complicated by the lack of an organized system for coordinating the planning and conduct of procurement, as well as ineffective feedback between the Armed Forces of Ukraine, the Ministry of Defense, and state business.

The use of a food catalog, which serves as the basis for buying food, presents another problem. Since there is no generally recognized mechanism for estimating the estimated cost, suppliers do set prices for each product unilaterally, which makes it difficult for the state to verify their legality. This makes it possible to manipulate prices, especially inflating prices for the most popular goods, advertising the lowest price for what is not ordered. This technique, together with the opacity of calculating the cost of catering services, makes it possible to abuse the official position when signing contracts and creates obstacles for new suppliers.

To reduce the impact of human factors on the development of applications and prevent abuse in the field, public experts have repeatedly called for reforming the food system, in particular for the separation of logistics services from food procurement processes and the introduction of seasonal menus (Antonyuk, 2023).

It is advisable to cite as an example of the current state of defense procurement, the example of the Ukrainian practice of "Egg Scandal". When it turned out that the Ministry of Defense had signed a contract for the supply of eggs at an inflated cost (two to three times higher than the market), in January 2023 a corruption scandal broke out with the purchase of food for the military. Journalists collected supporting documentation and reported facts contrary to martial law. The lack of proper internal control was revealed after additional studies since the responsible persons did not study the market conditions and did not check the accuracy of the supplier's figures. This example demonstrated that in the absence of reliable protection, the danger of inflated costs persists even in cases where procurement is extremely urgent. As a result, the Ministry of Defense began a review of internal pricing processes, and several officials were removed from their posts.

Under the conditions of martial law, the Ministry of Defense of Ukraine has identified serious systemic problems that not only indicate the inefficient management of state resources but also threaten the proper provision of military personnel, which directly affects the state's ability to defend itself. From the very beginning of the full-scale invasion of the Russian Federation, Ukraine had to urgently reconsider the issue of supplying troops. However, the system continued to rely on outdated Soviet processes of bureaucracy, centralization, and irresponsibility rather than moving to a new model of prompt, transparent, and responsible delivery.

One of the most obvious problems was the lack of a single relevant database that would reflect the real needs of military units. Objective information from the front was sometimes not taken into account when choosing material values; in particular, unit commanders were not properly informed of shortages or oversupply. Instead, purchases were often made in response to unstructured demands that arose through the chain of command, or for the remaining funds that needed to be "mastered" by the end of the budget period. As a result, millions of assets were purchased that did not meet the real needs of soldiers, climatic circumstances, or the details of conflicts (Pakhachuk et al., 2025).

In addition, the logistical aspect of providing the actual things remained a very weak point. The acquired assets were distributed slowly, often with months of delays and without a clear process. While centralized warehouses kept surplus purchased goods, often of unknown quality, fighters on the front lines were left to fend for themselves in search of uniforms, shoes, thermal underwear, personal hygiene products, and cold and rain protection components. The lack of a computerized accounting and control system made it difficult to monitor the number, movement, and exact position of assets. A favorable atmosphere for manipulation and abuse was created by the lack of clear instructions in the Ministry of Defense for keeping records in a combat situation and the fact that many units did not keep paper records at all, let alone electronic systems.

Even though certain contracts for the provision of physical property were signed with the understanding that payments would be made in advance, there was not enough control over the performance of contractors' duties. In addition to the fact that suppliers were not financially responsible, suppliers who did not produce property of acceptable quality or overdue deadlines nevertheless received new orders, sometimes at excessively high rates. Contracts were signed with enterprises that seemed fraudulent or did not have the necessary skills to perform such duties. Artificially high prices were the result of a lack of competition in the supplier market, which is especially risky with a limited budget (Shkola & Bakin, 2024).

Another aspect of the problem is the lack of internal control within the Ministry of Defense. There is hardly any system that would guarantee compliance with the terms of contracts, and even in situations of gross violations, the parties concerned are not subject to criminal or disciplinary penalties. Reports of the State Audit Service or internal audits that document many abuses rarely lead to systemic improvements. In addition, the system of the Anti-Corruption Committee of the Ministry of Defense was ineffective; despite numerous high-profile disclosures in the media, decisions regarding responsible persons were either delayed or ignored altogether.

All this points to a serious systemic problem of material support of the army. Every mistake, every pair of shoes or clothes detained during the conflict endangers the life of a serviceman. In addition, it becomes a national security problem, not just a problem of bad governance, when corruption or managerial errors lead

to such results. All stages of the process, from supply, logistics, and contract control to procurement planning and collecting demand from the front, must be quickly reformed by the Ukrainian government. Apart from the fact that transparency, digitalization, public accountability, and punishment of perpetrators are essential for effective governance, they are also core components of the nation's defense capability.

Equally important is the creation of an audit and internal control system. These procedures began to take shape in Ukraine in 2015, but serious shortcomings were revealed during the audit of public procurement in 2024. Problems with risk management and supplier assessment, in particular, indicate the need for significant development of institutional capacity and changes. The actual application of regulatory requirements will continue to be insufficiently effective in the absence of systemic adjustments. Good achievements are associated with the creation of state enterprises DOT and AOZ, which perform the duties of the state customer. If given institutional autonomy, and a proper compliance-control board, they can turn into useful tools for implementing procurement policies. However, at the moment there is a possibility that the active positions of these companies may be attacked, especially due to political influence and cyber threats, so it is necessary to strengthen their organizational and security stability. In the future, Ukraine should create a single national defense procurement organization, which would include both military and civilian experts, to coordinate a strategy in the field of security and defense (Rusina, 2025). Table 1 includes the dynamics of investigations, corruption cases, budget losses, digitalization, anti-corruption audits, and other key indicators of Ukraine's defense procurement.

**Table 1. Dynamics of corruption risks, losses and digitalization in Ukrainian defense procurement (2021–2025)**

| Year | Number of investigations | Loud cases | Budget losses due to violations | Number of audits | Level of digitalization | TI and NACP reports | Number of implementations | Number of suspensions |
|---|---|---|---|---|---|---|---|---|
| 2021 | 15 | - | 0.9 | 5 | 15 | 3 | 0 | 2 |
| 2022 | 22 | 5 | 1.5 | 9 | 20 | 6 | 1 | 5 |
| 2023 | 35 | egg scandal | 2.7 | 18 | 28 | 9 | 2 | 8 |
| 2024 | 50 | bulletproof vests | 3.4 | 26 | 40 | 12 | 3 | 12 |
| 2025 | 40 | ammunition | 2.5 | 22 | 50 | 11 | 4 | 10 |

Source: based on Rusina (2025)

Thus, corruption risks in defense procurement are the result of deeper systemic problems with organizational structure, regulatory uncertainty, duplication of authority, lack of a unified strategy, and poor planning, as well as individual violations or dishonest officials. The only way to reduce the level of misuse and guarantee the effective and fair use of budget funds in the defense sector is a complete reform based on the ideas of accountability, transparency, distribution of power, and institutional stability. Solving complex problems and relying on world experience are also crucial. The effectiveness of financial control systems, the verification of abuse, and the division of responsibilities between prevention and detection of violations are of particular importance during martial law. Significant budget funding for defense procurement and the huge potential for financial abuse make this issue even more urgent. Thus, in addition to studying institutional reforms, it is crucial to study real examples of financial investigation tools and oversight processes that can be modified by Ukrainian conditions.

The purchase of lower body armor by the Ministry of Defense, which caused

widespread public outrage, is one example of a successful financial investigation in Ukraine. The purchase of almost 11 thousand defective Corsair body armor, which did not meet the criteria for protection and could be fatal for military personnel, was published by the State Bureau of Investigation in 2019-2020. Despite what was known about the flaws, Department of Defense leadership accepted batches for registration despite ballistic analysis that confirmed the devices failed bullet testing. The possibility of real prosecution in defense procurement was demonstrated when the case went to trial and some of the defendants were dismissed.

Ukraine may adopt some aspects of foreign processes, such as the European Anti-Fraud Office (OLAF), the Government Accountability Office (GAO) in the United States, or the Defense Contracts Audit Agency (DCAA), to increase the effectiveness of controlling defense procurement costs. OLAF conducts both documentary and digital checks and conducts impartial investigations of fraud with EU budget funding. The GAO conducts a thorough analysis of state budget expenditures and issues conclusions that Congress must adhere to. To regulate the financial capacity and cost of the contractor, the DCAA reviews Pentagon contracts before they are completed. Financial investigations are reactive tools for responding to already identified signs of corruption or fraud to document, identify, and prosecute cases. This is in contrast to compliance procedures, which focus on preventing violations (through internal controls, integrity policies, and transparency).

As a structural component of a collective security strategy, NATO places a high priority on risk management in defense procurement. In the context of collective defense, where several countries can participate in joint production or use defense capabilities, risk management goes beyond the internal operations of one state and becomes an important prerequisite for interstate trust, standardization, and cost-effective use of public funds. The most important source in this area is the ARAMP-1 (NATO Risk Management Guide for Acquisition Programs), a comprehensive guide that describes the risk management procedure in the management of defense programs and procurement. From formulating requirements, evaluating alternatives, developing and testing to delivery, maintenance, and decommissioning, it covers the full project life cycle. It is important that in addition to broad recommendations, the ARAMP-1 describes in detail the duties and responsibilities of each party, the frequency of inspections, the risk analysis structure (for example, the

probability/impact matrix), and the response criteria. This strategy guarantees the uniformity of procedures between NATO members, which is especially important for initiatives that are funded or developed jointly and require joint risk assessment and management (Zhuravel, 2024).

Large-scale NATO initiatives, such as the NATO Alliance Ground Surveillance Program (AGS), a joint unmanned reconnaissance system based on the RQ-4 Global Hawk UAV, use ARAMP-1. In addition to pooling the resources of NATO's 15 members, the initiative has taken on significant risks related to cyber defense, real-time data sharing, technology integration, and a multi-year service cycle. Each risk was recorded in a centralized registry and monitored by the joint program management team. Digital risk monitoring modules have also been used in the NATO Support and Procurement Agency (NSPA) program for the maintenance of the A330 MRTT (Multi-Role Transport Aircraft and Refueling Aircraft), focusing on upgrade timelines, maintenance availability, and life-cycle cost control.

It is important to note the function of digital technologies, which are now a key component of NATO's modern risk management system. To predict delays or cost overruns, member countries are increasingly using integrated platforms that include risk registers, contract calendars, budgets, terms of reference, delivery schedules, and analytical modules. In some situations, a centralized project management system is used, such as the MRTT multinational fleet project, to which national representatives of the participating countries have access. This allows you to see the status of implementation in real time, identify critical points, and agree on an action plan without unnecessary bureaucracy. This is an illustration of how digital technologies enable full interaction between states (Baillie et al., 2024).

Although the phrase of anti-corruption compliance is rarely used in Alliance documents in a restrictive sense, NATO places a high priority on the unity of approaches to compliance and integrity. However, supplier enterprises must have internal controls, quality assurance, incident recording, feedback, and response procedures to meet the requirements of the AQAP (Allied Quality Assurance Publications) series of standards, in particular AQAP-2070 (Risk Management). Contracts with the NATO Support and Procurement Agency (NSPA), for example, require suppliers to undergo pre-qualification, which involves not only technical and financial assessment but also verification of their internal policies regarding corporate governance, conflict of interest, processing of confidential

information, and security of supply. Companies may not be allowed to participate in tenders at the Alliance level if they do not have such rules or do not comply with them (Shterma et al., 2025).

To ensure compliance with Alliance rules, NATO member states also use mirror control organizations. For example, the UK Ministry of Defense's Commercial Toolkit contains the necessary rules to curb corruption in all defense procurement. These rules include computerized forms for monitoring transactions, forms for declaring conflicts of interest and publishing contractor integrity policies. Important defense initiatives in Denmark are monitored by the Ministry of Defense's Audit and Risk Management Committee through a consolidated online platform, and the committee's findings are subject to legislative review.

Germany is introducing a digital portal for reporting costs and risks in defense procurement, the EBAU system (Elektronisches Berichtswesen für Ausrüstung und Unterstützung). It is also used to assess compliance with NATO standards. These examples show that risk management, compliance, and digital audit are not formally separated in the Alliance; rather, they are all seen as part of a single procurement security logic, with digital platforms serving as the primary tool for implementing traditional procedures rather than as an adjunct to them. Therefore, in addition to the formal study of ARAMP-1 or AQAP, Ukraine must also build the necessary digital infrastructure, train staff and create institutional conditions for the real use of these tools in the framework of adaptation to NATO standards (Antonyuk & Zinko, 2023).

The experience of the United States and the EU, which are members of NATO, should also be taken into account. This decision was made for several reasons. First, these countries interact with our defense structures most often through international initiatives and are the main suppliers of security assistance to Ukraine. Second, their defense procurement systems are extremely advanced, have evolved over the years, and now represent the highest international standards of digital transformation, risk management, and financial control. Thirdly, Ukraine's approach to the Alliance's standards is influenced by the experience of the United States and the European Union, which is directly included in the NATO regulatory framework and standards (namely ARAMP-1, AQAP, and STANAG). The study of these models makes it possible to choose exactly those tools that can be adapted to Ukrainian realities, taking into account the current

difficulties, martial law, lack of resources, and the requirement for operational but balanced decisions. It also helps to better understand how risk management functions in practice under democratic civilian control (Petrunyak, 2023).

Anchored in FAR, DFARS, and specialized recommendations such as the Risk Management Guidelines for Defense Procurement Programs, risk management in defense procurement is a key component of the United States planning and contracting system. The criteria stipulate that risk management should be included in each phase of the program life cycle, from the definition of operating requirements. All program participants - managers, engineers, and contractor employees - should maintain risk registers, assess the likelihood and impact of risks, appoint those responsible for mitigating them, and carry out ongoing monitoring.

This is achieved through the active use of digital technologies, namely the Earned Value Management technique, which allows you to detect temporary and financial aberrations in advance. Legislative safeguards, such as the Anti-Deficit Act, which prohibits spending beyond allocated funds and establishes personal responsibility, and the Nunn-McCurdy Amendment, which mandates reporting to Congress in the event of significant spending overruns, provide additional discipline. Strong external control is another key component of American strategy: independent inspections of defense contracts are conducted by the Defense Contracts Audit Agency and the Government Accountability Office, which also confirm costs and detect inefficiencies and fraud (Makarenkov & Kosa, 2024).

The United States is experiencing a systemic digitalization of defense procurement. Well-known platforms such as SAM.gov and PIEE (Procurement Integrated Enterprise Environment) automate the processes of announcing, concluding, and monitoring contracts, as well as offering real-time control, analytics, and access to historical data. High-precision audits are made possible by integrating data with other information systems. Contractors must simultaneously have anti-corruption compliance strategies, including integrity rules, internal control systems, conflict of interest detection processes, and frequent training of personnel. The danger of corruption, collusion, or financial abuse is greatly reduced by such programs, which are checked both during the selection process of the supplier and during the execution of the contract. Internal processes, digital technologies, external audits, and years of institutionalized experience in managing defense contracts form the basis of the entire US system (Stetsenko, 2025).

In the EU, competitiveness, openness, and compliance with standardized rules are directly related to risk management in defense procurement. The general European criteria for defense tenders are laid down by the 2009/81/EC Directive, namely on open procedures, even in the style of negotiation, and mandatory public statements on proposed procurement. While allowing national security interests to be taken into account, the directive also introduces several safeguards, including flexible but regulated competitive procedures, requirements for the security of supply and protection of classified information, special conditions for research and development, and mechanisms for promoting competition in supply chains, in particular through the obligation to engage subcontractors (Mik, 2024).

One of the most important risk mitigation tools in modern EU practice is digitalization. Electronic defense procurement systems that offer automatic review of tenders, reporting, submission, and announcement of tenders are used in many countries. Electronic registries of suppliers and contracts made it possible to track previous performance, identify systematic problems, and avoid duplication of procurement and collusion. The best exchange of data between national procurement agencies, in particular about unscrupulous suppliers and cases of collusion on tenders, is facilitated by the assistance of the European Commission in the development of standard IT systems.

Compliance with anti-corruption legislation is also crucial. Firms bidding for contracts must adhere to moral principles, report no conflicts of interest, and show they are a well-run company. Integrity rules, internal controls, and protocols for reporting violations are part of the internal compliance processes that many countries require of contractors. Accounting chambers, inspections, special agencies, and antimonopoly bodies exercise constant control at the federal level. For example, Germany's defense contracts worth more than 25 million euros require parliamentary approval, which guarantees political and financial supervision, while the UK has an independent regulator, SSRO, which monitors the price of non-gender contracts (Kussainov et al., 2023). Although the European model is less technically unified, it is based on the same ideas: interstate cooperation, digital surveillance, legal responsibility and transparency of procedures. Competition, electronic tools, and compliance programs create a tiered system to stop abuse and reduce the risk of monopolization, corruption, and waste.

*Discussion*

Ukraine is aggressively changing the structure of defense procurement, which is especially important now when a full-scale conflict is brewing. The system is still susceptible to violations and needs a systematic rethinking, even with the adoption of the new Law "On Defense Procurement" and the creation of specialized organizations such as the State Defense Procurement Agency, the Logistics Agency of the Ministry of Defense and the Anti-Corruption Council under the Ministry of Defense. Inadequate digitalization of processes, poor integration of risk management mechanisms into real activities, and inconsistent implementation of the anti-corruption compliance program by the government and suppliers are among the main obstacles.

The most illustrative are cases where formal contractor due diligence procedures lead to the signing of contracts without taking into account objective risks. As an example, consider the case of the purchase of ammunition in 2023, when the corporation did not have enough production capacity, and the product was faulty. Despite the overall risk management criteria, no thorough supplier analysis, technical audit, or financial assessment has been carried out, suggesting a lack of an organized approach to due diligence. Such errors have serious consequences during the war, not only in terms of monetary losses but also because they can directly jeopardize the combat capability of defensive forces (Sobko et al., 2023).

In this regard, the digitization of defense procurement should serve as the basis for the implementation of the most modern standards of risk management, accountability, transparency, and integrity, and not just an automation tool. The first step is to create a single digital cycle that integrates every stage of the procurement process, from planning and analyzing requirements to monitoring contract performance. The creation and adoption of departmental regulations (guidelines) on risk management in defense procurement that meet the NATO ARAMP-1 standard is an important first step. Clear guidance on identifying risks, assessing their effect and likelihood, appointing responsible parties, deciding on appropriate response measures, establishing risk registers, and tracking them over time should be included in such a document. These processes should be incorporated into a digital platform that provides status tracking, analysis of important supply chain points, and real-time risk collection and updating. With data visualization, automated risk indicators, and links to financial and contract data, such a system

should serve as a dashboard for the leadership of the Department of Defense, defense departments, and regulatory agencies. In addition to improving the quality of managerial choices, this will result in individuals being held accountable for their inaction in response to identified dangers (Astramowicz-Leyk et al., 2023).

For non-classified categories, it seems appropriate to simultaneously restore and expand the use of electronic procurement. Having developed a separate module for military procurement with limited access and open fields for important information (product category, quantity, term, and selected supplier), the Prozorro system can already be modified for defense needs. The introduction of such a module will significantly reduce the likelihood of overpricing, collusion, and discrimination of competitors. In addition, analytical methods for assessing supplier integrity should be incorporated into digital systems. These tools should be based on the past participation of suppliers in tenders, the number of terminated contracts, the frequency of victories in the same procedures, and the presence of corruption scandals. Methodical application of anti-corruption compliance should be the main direction of action. This involves not only the creation of official anti-corruption units but also ensuring that participants in defense tenders have independent internal investigation procedures, personnel training, methods of preventing conflicts of interest, and internal rules of integrity. Companies with a dubious reputation or opaque ownership structure may be prohibited from participating if the relevant criteria are included in the tender documentation and automatically verified by an integrated database.

Ukraine should take measures to create an autonomous department for auditing defense contracts at the institutional level. This unit can operate at the Accounts Chamber, the State Audit Service, or even as a separate organization (like the US DCAA). Such a unit should have access to all data of digital contracts, have the technological capabilities to conduct a thorough study of pricing, monitor the correspondence of value to market levels, and identify evidence of collusion or inflated margins. A parliamentary report on the risks of defense procurement could be implemented in the future. The Ministry of Defense will report quarterly or half-year to the Verkhovna Rada Committee on National Security on the most risky programs, complex contracts, and the implementation of previous recommendations (Sanders, 2023). Institutional growth must go hand in hand with digital change. Training on risk management, digital procurement analysis, and compliance should be provided to Ministry of Defense and Defense

staff. This could include unique courses modeled on Ukrainian anti-corruption organizations, training under NATO programs, or Twinning partnerships with EU countries. The training should include both fundamental modules and specific topics such as data analysis, anomaly detection, creation of a monitoring system, and information visualization.

Equally important is the participation of international partners in the development of a single digital infrastructure. G7, EU, and NATO countries through the Comprehensive Assistance Package (CAP) offer ready-made solutions (information platforms, compliance modules, and risk analysis algorithms) that can be adapted to the needs of Ukraine. It is crucial to include foreign aid in current or new digital procedures rather than creating parallel systems. For example, in addition to methodological assistance, the European Defense Agency, the European Anti-Fraud Office (OLAF), and UK defense spending control institutions may offer access to uniform supplier registers, risk indicators, and price anomaly monitoring procedures (Poliova et al., 2024).

In addition to technical cooperation, it is critical to ensure institutional independence and political support for the digital transformation of defense procurement. Only if advanced digital technologies truly influence decision-making, access to complete contact information, and protection from administrative or political pressure can such changes be successfully implemented. For this reason, digital technologies and parliamentary and public monitoring procedures should act in tandem. Public anti-corruption groups such as TI Ukraine and NAKO, as well as the relevant committee of the Verkhovna Rada, can become valuable employees in overseeing the implementation of new policies and practices.

In light of the above, we can say that for the effective adaptation of international standards in the field of military procurement, they must be divided into those that can be fully, partially, or only after significant modification applied in Ukraine. Using this method, the danger of formal use of models that do not meet the requirements of martial law, limited resources, and institutional capabilities is avoided. Individual provisions of the ARAMP-1 (such as the risk assessment matrix and the principles of responsibility allocation) and components of the AQAP-2070 (such as feedback mechanisms, incident management, and internal control of suppliers) are now among the standards that can be applied in practice. Including them in internal instructions for clients or as a necessary qualification

for contractors is a good idea.

Through the development of a digital contract database, pricing monitoring modules, and performance analytics, other standards such as DCAA audits or GAO reporting can be gradually implemented. Since the full implementation of such technologies requires the training of personnel and the creation of technological infrastructure, this is possible in the middle of the future. Last but not least, some standards, which are based on long-term budgeting, legislative reports, and complex multilevel verification (as in the US or Germany), can be used as benchmarks for the future, but cannot be adopted immediately. By using a clear implementation strategy, you can avoid unnecessary bureaucracy and focus on making changes that are feasible and useful right away.

To sum up, the new defense procurement system should have a unified integrated design that will include digitization, risk management, and anti-corruption compliance, rather than individual changes. Transparency, predictability, digital reporting, and automated controls to stop abuse should be its cornerstones. In addition to increasing domestic trust in Ukrainian institutions, this strategy will increase the effectiveness of the use of foreign military assistance, accelerate the country's integration into Euro-Atlantic institutions and, over time, strengthen its defense capability.

## *Conclusions*

We need a comprehensive structural restructuring of Ukraine's defense procurement system with an emphasis on digital transformation, systemic risk management, and the introduction of modern anti-corruption compliance initiatives. Despite this, it is sensitive to inefficiency, corruption threats, and reduced trust from both local and foreign partners, even after a series of changes and the creation of new institutions. This scenario is especially risky during a full-scale conflict when the ability of a state to defend itself depends on the efficiency, caliber, and integrity of its supplies.

Contemporary problems, in particular the need for rapid decision-making without compromising accountability, the need for openness without compromising secrecy, constant price fluctuations, and logistical difficulties, are all problems that the existing paradigm does not solve. However, the organizational structure of the Ministry of Defense is still too centralized, departments perform duplicate

tasks, responsibilities are not clearly defined, and digital technologies are used inconsistently. Delays, overpricing, inefficient use of resources, and arbitrary judgments that are often not properly controlled are all made possible by this.

Only a comprehensive risk management system built on digital analytics, transparency, and compliance can guarantee the effectiveness of defense procurement, as demonstrated by the experience of NATO member countries, including the United States and the EU. Risk registries, centralized supplier databases, real-time audit systems, and mandatory internal integrity rules are all included in the computerized platforms of these countries. They reduce the human factor, identify violations in advance, and ensure that everyone involved in the process is held accountable.

With the adoption of the Law "On Defense Procurement", the creation of specialized institutions, and the political will to change, Ukraine already has the foundation for the implementation of these strategies. Only by moving to a comprehensive digital architecture, from planning to contract execution, can we make further progress. It is necessary to introduce mandatory risk assessment at all stages, digital registers of decisions and risks, independent audits with access to all data, and make the availability of anti-corruption compliance programs for suppliers a mandatory requirement for participation in tenders. Political support, involvement of foreign partners, and development of institutional capacity for their implementation are necessary for these reforms to be successful.

In addition to eliminating the possibility of corruption, a thorough review of the defense procurement system should increase the efficiency of the use of resources, strengthen the country's defense capability and attract sponsors and friends. This is especially true in the light of future Euro-Atlantic integration, when compliance with global norms of accountability, openness and integrity is an extremely important requirement.

Integrating digital technologies into a unified and comprehensive process is crucial for minimizing risks and ensuring accountability across all stages of defense procurement. This approach underscores the direct relationship between digitalization and the mitigation of corruption risks, emphasizing the need for a holistic implementation from initial planning to final reporting rather than a phased or fragmented one. At the planning stage, integration with logistics databases and real-time information from the front line enables the Armed Forces of

Ukraine to collect and assess needs based on verifiable data rather than subjective administrative or political considerations. The use of analytical modules at this stage facilitates the prediction of shortages, prevents duplication of orders, and curbs unjustified budget expenditures.

During the tender announcement phase, digital systems enhance transparency by clearly presenting conditions and automatically verifying conflicts of interest, contractor histories, and potential corruption threats. When qualification requirements and bids are published through open API electronic platforms, the opportunities for manipulation in supplier selection are significantly reduced. In the evaluation of bids, algorithmic tools help identify inflated or irrational pricing by cross-referencing proposed costs with current market rates and automatically flagging anomalies. These systems also integrate with contractor registries to ensure that only qualified and compliant participants are considered.

Supply control is strengthened through real-time digital tracking of delivery statuses using geolocation data and unique identifiers. This allows for visualization of supply chain bottlenecks and generates automatic alerts in the event of delays, thereby reinforcing supplier accountability. Finally, the phase of contract support and audit is enhanced through the integration of contracts with risk registries, integrity indicators, financial monitoring systems, and independent analytical platforms accessible to the Ministry of Defense and legislative oversight bodies. This infrastructure enables the early detection of violations before they escalate. By embedding verification mechanisms throughout the entire procurement process, digital integration reduces reliance on manual decision-making, diminishes the influence of human error or bias, and significantly improves the legitimacy and reliability of each purchase.

## REFERENCES

Antonyuk, N., & Zinko, I. (2023). Cooperation between Ukraine and the European Union within the framework of the Common Security and Defense Policy of the EU. *Language – Culture – Politics, 1*(1), 247–270. https://doi.org/10.54515/lcp.2023.1.247-270

Antonyuk, O.I. (2023). *Interaction between government bodies and the private sector in combating corruption under martial law in Ukraine.* Chernivtsi: Yuriy Fedkovych Chernivtsi National University.

Astramowicz-Leyk, T., Nagornyak, T., Natalina, N., Osmolovska, A., & Yurkovsyi, V.

(2023). Anti-corruption policy in Ukraine during the war with Russia. *Prawo i Więź, 3*(46), 551-575. https://doi.org/10.36128/PRIW.VI46.660

Baillie, L., Dion, E., Leroux-Martin, P., Platz, I., Taylor, W.B., & Trenkov-Wermuth, C. (2024). *The future of the security sector in Ukraine.* Washington: United States Institute of Peace. Retrieved from https://eurasia.ro/wp-content/uploads/2024/10/future-security-sector-ukraine.pdf

Kussainov, K., Goncharuk, N., Prokopenko, L., Pershko, L., Vyshnivska, B., & Akimov, O. (2023). Anti-corruption management mechanisms and the construction of a security landscape in the financial sector of the EU economic system against the background of challenges to European integration: Implications for artificial intelligence technologies. *Economic Affairs, 68*(1), 509-521. https://doi.org/10.46852/0424-2513.1.2023.20

Makarenkov, O., & Kosa, V. (2024). Forensic Technique for Identifying Corruption Challenges to National Security through Digital Technologies. *Baltic Journal of Economic Studies, 10*(4), 288-300. https://doi.org/10.30525/2256-0742/2024-10-4-288-300

Mik, T.B. (2024). Corruption in defense procurement: Key threats and mechanisms to overcome them to ensure the national security of Ukraine. *Effectiveness of Public Administration, 1*(78/79), 71-76. https://doi.org/10.36930/507811

Pakhachuk, Ya.Y., Abramov, A.P., & Cherevatyi, T.V. (2025). Prospects for implementing foreign risk management experience in Ukrainian defense procurement legislation. *Achievements of the Economy: Prospects and Innovations, 14*, 1-25. https://doi.org/10.5281/zenodo.15023442

Petrunyak, E.V. (2023). Anti-corruption program as the basis of counteracting corruption in the financial sector. *Academic Visions, 26*, 1-8. https://doi.org/10.5281/zenodo.14950177

Poliova, N., Polova, L., Stepanenko, S., Izmailov, Y., Varenyk, V., & Akimov, O. (2024). Organizational and economic principles of financial monitoring of national business entities in the context of national security. *Edelweiss Applied Science and Technology, 8*(6), 1455-1466. https://doi.org/10.55214/25768484.v8i6.2262

Rusina, Yu.O. (2025). State financial control: Martial law period main challenges. *Actual Problems of Economics, 2*(284), 148-160. https://doi.org/10.32752/1993-6788-2025-1-284-148-160

Sanders, D. (2023). Ukraine's third wave of military reform 2016–2022 – Building a military capable of defending Ukraine against the Russian invasion. *Defense & Security Analysis, 39*(3), 312-328. https://doi.org/10.1080/14751798.2023.2201017

Shkola, V.Yu., & Bakin, M. (2024). In V.Yu. Shkola, & M.D. Domashenko (Eds.), *Mechanisms for countering modern challenges and threats: EU experience for Ukraine: Materials of the international scientific and practical conference* (pp. 197-200). Sumy: Sumy State University. Retrieved from https://essuir.sumdu.edu.ua/handle/123456789/96627

Shterma, T.V., Lukivskyi, A.S., & Lukivskyi, S.D. (2025). Introducing artificial intelli-

gence into economic management models to minimize corruption risks. *Achievements of the Economy: Prospects and Innovations, 15*, 1-22. https://doi.org/10.5281/zenodo.14959270

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. https://doi.org/10.14718/NovumJus.2023.17.2.9

Stetsenko, I. (2025). Experience of NATO countries and Ukrainian realities regarding the activities of counterintelligence agencies in the state system of information security assurance. *Global Scientific Trends: Economics and Public Administration, 1*(1), 47-56. https://doi.org/10.5281/zenodo.14812097

Transparency International. (2024). Corruption perceptions index. Retrieved from https://www.transparency.org/en/cpi/2024

Zaremba, O.O., & Lusta, A.A. (2021). Anti-corruption audit as a factor of economic growth of the country. In *Modern directions of scientific research development: Proceedings of VI international scientific and practical conference* (pp. 921-925). Chicago: BoScience Publisher.

Zhuravel, V.V. (2024). *Public finance management in wartime.* Zaporizhzhia: Zaporizhzhia National University.


Breastplate of the Ukrainian Ministry of Defense
Author: Олекса Руденко 1990. Public Domain
Wikimedia Commons

# Special Dossier October 2025
## *Ukraine Military and Wartime Law*

*Articoli / Articles*