

TPO^{2.0}

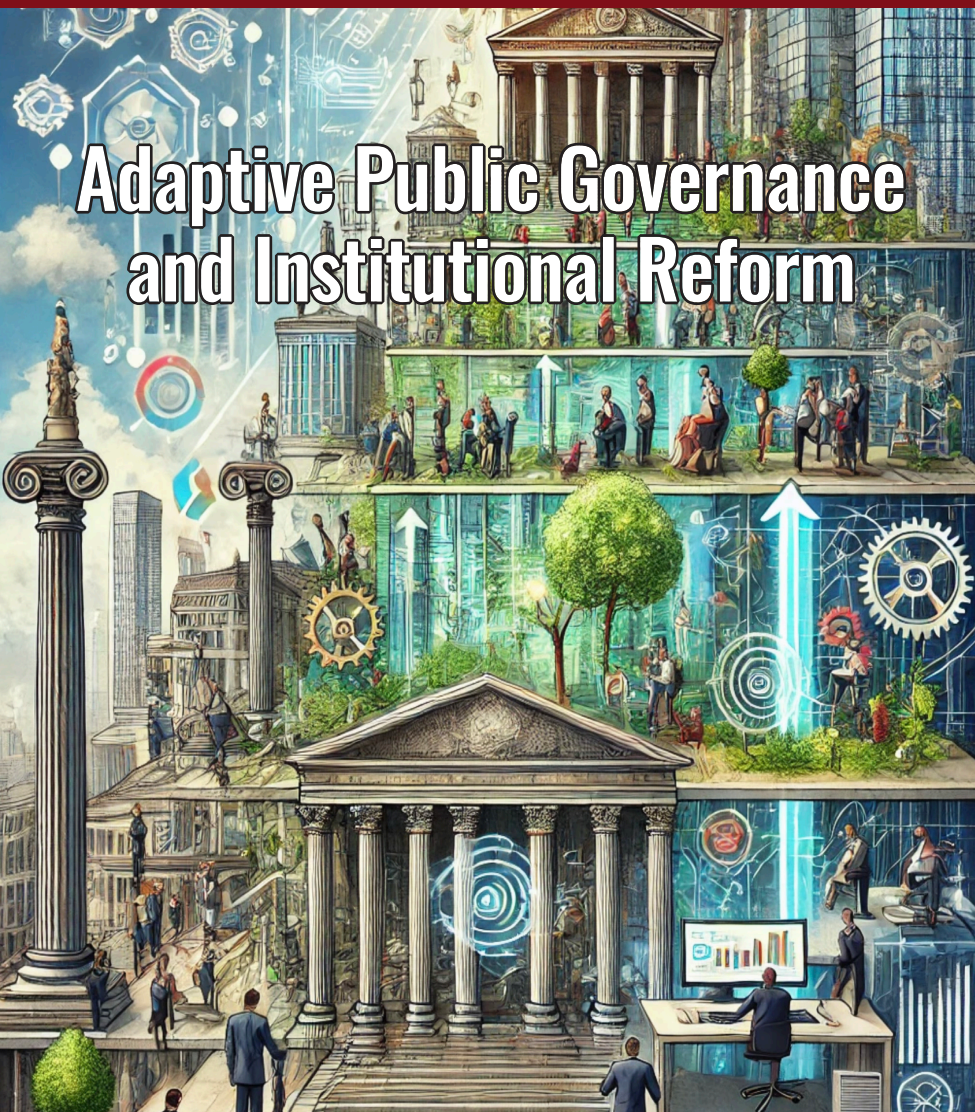
Transatlantic Policy Quarterly

• Spring 2025 • Vol. 23 • No. 4 •



ISSN: 2822-373X

Adaptive Public Governance and Institutional Reform



Lazar Comanescu
Promoting Resilience
and Prosperity in the
Wider Black Sea Region
and the Role of BSEC

Emre Karter
Adaptive Governance in
Global Business:
Strategic Resilience
Through Spatial, Digital,
and Human Capital
Integration

Nataliia Veresniuk,
Dmytro Lavrentii,
Grygorii Monastyrskiy,
Yaroslav Demchyshyn
& Yana Levytska
Reforming Healthcare:
Challenges in Public
Administration and
System Overhaul
Reforming Healthcare

• Alina Pomaza-Ponomarenko • Dmytro Taraduda • Oleh Kravchuk • Svitlana Moroz •
• Olena Akhmedova • Stanislav Poroka • Oleksandr Skrypniuk • Nataliya Onishchenko •
• Mykhailo Nonyak • Serhii Sunegin • Tetiana Shestakovska • Olena Mykhailovska •
• Oksana Liashenko • Hanna Chumakova • Nataliia Filipova • Sergey Grivko • Yurii Dziurakh •
• Nazar Podolchak • Natalia Tsygrylyk • Veronika Karkovska • Olena Bilyk • Oleh Sokil •

TABLE OF CONTENTS

8	Aybars Arda Kılıçer Adaptive Public Governance and Institutional Reform
10	Lazar Comanescu Promoting Resilience and Prosperity in the Wider Black Sea Region and the Role of BSEC
16	Emre Karter Adaptive Governance in Global Business: Strategic Resilience Through Spatial, Digital, and Human Capital Integration
26	Nataliia Veresniuk, Dmytro Lavrentii, Grygorii Monastyrskiy, Yaroslav Demchyshyn & Yana Levytska Reforming Healthcare: Challenges in Public Administration and System Overhaul
38	Alina Pomaza-Ponomarenko, Dmytro Taraduda, Oleh Kravchuk, Svitlana Moroz, Olena Akhmedova & Stanislav Poroka National Security Management: Organizational, Legal, Informational, and Human Resource Dimensions

50

Oleksandr Skrypniuk, Nataliya Onishchenko,
Mykhailo Nonyak & Serhii Sunegin

**Peace as a Fundamental Human Right: The Progression of its
Content and Future Potential**

66

Tetiana Shestakovska, Olena Mykhailovska, Oksana Liashenko,
Hanna Chumakova, Nataliia Filipova & Sergey Grivko

**Promoting Community Prosperity by Overcoming Gender and
Migration Challenges**

80

Yurii Dziurakh, Nazar Podolchak, Natalia Tsygylyk, Veronika
Karkovska, Olena Bilyk & Oleh Sokil

**Applying Design Thinking to Help Public Servants Overcome
COVID-19 Challenges**

NATIONAL SECURITY MANAGEMENT: ORGANIZATIONAL, LEGAL, INFORMATIONAL, AND HUMAN RESOURCE DIMENSIONS

DOI: 10.58867/IKHU8222

Among the main problems of modern social transformations, public administration in the field of national security plays an important role. Against the backdrop of wartime threats and social instability, critical risks require mobilizing organizational, information, human, and legal resources to ensure stability in the national environment. The study analyzes public administration's current organizational, legal, personnel, and information aspects that ensure national security. It examines the main possibilities of information, organizational, legal, and personnel support of national security. The principles of building a system of national security are highlighted. The main problems, challenges, and achievements of the information transformation of the security sector in the context of digitalization are analyzed.

Alina Pomaza-Ponomarenko, Dmytro Taraduda,

Oleh Kravchuk, Svitlana Moroz,

Olena Akhmedova, Stanislav Poroka

Keywords: National Security, Human Resource Management, Legal, Informational.



TPQ

Spring 2025

Adaptive Public Governance and Institutional Reform

* The complete affiliations of the authors are available in our website: <http://transatlanticpolicy.com/article/1293/national-security-management-organizational-legal-informational-and-human-resource-dimensions>

The national security development strategy is a system of organizational, regulatory, managerial, socio-psychological, educational, personnel, and information measures to ensure the observance of national interests. Implementation of the strategy in practice is achieved through the practical interaction of participants in the public administration process to prevent possible or potential threats that may interfere with the normal functioning of the national space due to the influence of external and internal factors.

The overall goal of the national security strategy is to create a stable basis for the unimpeded realization of national interests and effective counteraction to threats and dangers. In today's context, this goal is achieved through information, organizational, legal, and human resources. Given active digitalization, each of these aspects currently requires improvement.

Therefore, given current global challenges, the national security strategy needs to be updated and adapted, and a set of measures to guarantee it needs to be developed. This involves improving the efficiency of the sector's organizational, legal, personnel, and information support.

Literature Review

Modern scholars actively study the issue of public administration in the context of national security. Scientific publications are devoted to the functioning of innovative mechanisms of public administration,¹ subjectivisation of security policy and its regulation processes,² differentiation of functional areas of the security concept,³ and the functionality of information tools in the public administration system of national security.⁴

Thorough works⁵ present innovative approaches to national security management

1) V. Chalapko, "Information security: to the problem of place and role in the national security system", *Yaroslav the Wise NSW Bulletin. Series: Philosophy, Philosophy of Law, Political Science, Sociology*, Vol. 4, No. 51 (2021); O. Panchenko, "The role of the media in the system of public administration of information security", *Public Administration and Customs Administration*, Vol. 1, No. 24 (2020), p. 97-102.

2) S. Poterayko, "Problems of public administration of civil protection in ensuring state security of Ukraine", *Investments: practice and experience*, Vol. 9 (2021), p. 103-108.

3) I. V. Kukin "A comprehensive mechanism for public management of personal information security in the field of national security and its border sector", *Public Administration and Customs Administration*, Vol. 4, No. 27 (2020), p. 134-139.

4) A. Pomaza-Ponomarenko et al., "Management mechanisms in the context of digitalisation of all spheres of society", *Revista San Gregorio*, Vol. 42 (2020); Pomaza-Ponomarenko et al. "Managing emergencies: utilising historical insights for strategic enhancement", *AD ALTA: Journal of Interdisciplinary Research*, (2024), Vol. 14, No. 01-XLII, p. 135-139; A. Pomaza-Ponomarenko et al., "Ensuring the safety of citizens in times of war: aspects of the organisation of civil defence", *AD ALTA: Journal of Interdisciplinary Research*, Vol. 14, No. 01-XXXIX (2024), p. 216-220; E. K. Szczepaniuk et al., "Assessment of information security in public administration", *Computers and Security*, Vol. 90 (2020).

5) V. Zagurska-Antonyuk, "National security and public administration", *Galician Economic Herald*, Vol. 66, No. 5

using technological capabilities and digitalization. Several scientists in the modern national scientific space have significantly contributed to the general methodology of forming the concept of national security.⁶

The peculiarities of modernizing the systems integrated into the Digital State project are presented in the study by O. Skybun.⁷ Researcher I. Sopilko examines the regulatory and legal support for the information security system and highlights the need to harmonize the sectoral legislative framework in Ukraine in line with the requirements and norms of international standards.⁸ The researchers I. Revak and R. Gren⁹ investigate modern methods of practical combating cybercrime in the context of the state and corporate levels. S. Bondarenko et al., H. Sytnyk et al. study the specifics of improving the national concept of strategic planning for developing the national security sector in the context of society's informatization.¹⁰ At the same time, S. Dovgy et al.¹¹ analyse the impact of the "legitimacy crisis" on the information security of the state's system of public authorities.

The problems of the methodology of information protection in the public sector are addressed in the scientific works and publications of foreign scientists S. Rass et al. and M. Albahar.¹² Scientists emphasize the importance of ensuring cyber defense in the context of critical public infrastructure.

A number of scholars have considered certain issues of optimizing the organizational, legal, and institutional foundations of national security.¹³ Scientists thoroughly analyze

(2020), p. 187-193; O. Klochko & I. Semenets-Orlova, "National security: the Ukrainian dimension. Scientific works of the Interregional Academy of Personnel Management", *Political Science and Public Administration*, Vol. 2, No. 62 (2022), p. 66-75; T. Podkovenko, "National Security of Ukraine: Axiological and Legal Aspects", *Actual Problems of Jurisprudence*, Vol. 1, No. 1 (2020), p. 11-18.

6) Y. M. Pavliutin, "General theoretical dimension of national security as an object of public administration", *Honour and Law*, Vol. 2, No. 73 (2020), p. 115-121; F. Zhang, "Mechanisms for regulating the professionalisation of public service personnel in the context of European integration as a national security issue", *Public management*, Vol. 5, No. 33 (2022), p. 114-119; R. B. Primush, "Directions for increasing the effectiveness of public administration in the field of national security", *Economics, management and administration*, Vol. 2, No. 100 (2022), p. 44-48.

7) O. Zh. Skibun, "Cybersecurity of electronic communications systems of public authorities of Ukraine", *Visnyk of the National Academy of Public Administration. Series "Public Administration"*, Vol. 1, No. 100 (2021), p. 30-39.

8) I. Sopilko, "Information security and cybersecurity: a comparative legal aspect", *Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law"*, Vol. 2, No. 59 (2021), p. 110-115.

9) I. O. Revak I. O. & R. T. Gren, "Features of the formation of secure cyberspace in the context of the development of the digital economy", *Innovative Economy*, Vol. 3-4 (2021), p. 164-169.

10) Bondarenko et al., "Improving the State system of strategic planning of national security in the context of informatisation of society", *Journal of Information Technology Management*, Vol. 14 (2022), p. 141-24; H. P. Sytnyk et al., "Conceptual understanding of the peculiarities of managing innovation-driven development of the state in the current conditions", *Science and Innovation*, Vol. 18, No. 2 (2022), p. 3-15.

11) Dovgy, S. et al., "'Legitimacy Crisis' and its Impact on the Stability and Security of the System of Public Authorities of the State during the Formation of the Global Information Space", in *Contributions to Political Science*, (Springer Nature Switzerland AG, 2023), p. 237-256.

12) S. Rass et al., *Cyber-Security in Critical Infrastructures* (Springer International Publishing, 2020); M. Albahar "Cyber attacks and terrorism: A twenty-first century conundrum", *Science and engineering ethics*, Vol. 25, No. 4 (2019), p. 993-1006.

13) A. Babuta et al., *Artificial intelligence and UK national security: policy considerations. Technical Report*. (RUSI, London, 2020); E. H. Klijn & J. F. Koppenjan, "Public management and policy networks: Foundations of a network

the foundations of effective public administration in Ukraine's national security field, focusing on improving information and organizational support.

Researchers D. Mandel and D. Irwin¹⁴ study the issue of national security from the standpoint of uncertainty, which is especially relevant in the current environment. In continuation, N. Putro and M. Sirleaf¹⁵ position the phenomenon of national security as the basis for society's well-being, the country's competitiveness in the international arena, and the development of its influence. G. Dimitropoulos studies national security in the context of the role of investment verification mechanisms.¹⁶

Despite the significance of scholars' scientific and practical achievements on the issues under study, scientific research on the role of public administration in ensuring national security needs to be developed.

The study analyzes national security's current organizational, legal, personnel, and information public administration aspects.

Materials and Methods

The research materials were industry publications, materials from scientific and practical conferences on national security issues, and statistical data.¹⁷ At the same time, preference was given to modern developments in the current context of the digitalization of business processes and resource management.

The study uses a set of complementary general scientific theoretical methods, including analysis, synthesis, and abstraction. The integration of analysis and synthesis allowed for an objective and comprehensive study of the aspects of public administration in the context of national security. System analysis helped to clarify the essence of definitions and conceptual categories. Using synthesis, the individual components and properties identified based on the analysis were combined into a single whole. In this process, there was a meaningful combination in the direction from the identical and essential to differentiation and diversity, integrating both general and individual aspects into a single concept. The study used comparative analysis to assess the legal framework and regulatory and institutional support for national security, focusing on information security. Based on an understanding of global trends and practices, approach to governance", in *Making Policy Happen* (London, Routledge, 2020), p. 28-40.

14) D. Mandel, D. Irwin, "Uncertainty, Intelligence, and National Security Decisionmaking", *International Journal of Intelligence and CounterIntelligence*, Vol. 34, No. 3 (2021), p. 558-582

15) H. P. Putro, "Make a prosperous state through national security", in *International Conference on Law, Economics and Health* (ICLEH 2020) (Atlantis Press, 2020), pp. 328-334; M. Sirleaf (ed.), *Race and National Security* (Oxford University Press, 2023).

16) G. Dimitropoulos, "National security: The role of investment screening mechanisms", in *Handbook of international investment law and policy*, (Springer Nature, 2020), p. 1-37.

17) NCSI (National Cyber Security Index) Cybersecurity Rating for 2023 (2024) – available at. <https://ncsi.ega.ee/country/ua/>

the study compares the evolution of regulation in Ukraine with European standards while considering the contextual national specifics.

The research procedure included two main stages: data collection and analysis. In the first stage, we used primary data sources obtained through the analysis of industry statistics, regulations, and publications. This sample size was deemed reasonable in light of the practical realities that needed to be considered. The data was analyzed using mixed methods: quantitative and qualitative statistical analysis.

The abstraction method was employed to isolate theoretical generalizations, define the main categories and concepts, and formulate conclusions on the priority vectors of ensuring national security through human, information, organizational, and legal management resources. At the same time, the abstraction of potential practical feasibility was used as a mental distraction from the standard properties of management technologies, concepts, and tools, with the simultaneous highlighting of the essential properties sought.

Results

National security is aimed at avoiding existing and potential threats to the normal development of the state. Building the national security system should be based on the following basic principles:

- The principle of the priority of national interests;
- The principle of mutual responsibility of the individual, society, and the state;
- The principle of interaction and coordination between the state and non-state subsystems of national security, prompt information, and coordination of actions of the national security forces;
- The principle of providing the public with reliable information;
- The principle of responsibility of management entities and justified risk;
- The principle of adequate response, unity, and balance of all components of national security;
- The principle of openness to the positive international experience of organizing the national security system.

The qualitative features of the functioning of the national security system are the country's combat capability, mobility, controllability, awareness, efficiency, sustainability, resilience, and adequacy.¹⁸

¹⁸) Rass, S. et al., *Cyber-Security in Critical Infrastructures* (Springer International Publishing, 2020).

Organizational and Legal Public Administration Aspects in the Sphere of National Security

Organizational and Legal Public Administration Aspects in the Sphere of National Security are the governing legal information for the functioning of the security system, the sources of which are the Constitution of Ukraine, laws, and other regulatory legal acts. These normative resources determine the functionality and tasks of the national security actors (state and non-state) in general and specific vectors of their activity by levels of management and subsystems.

The actors implementing the national security strategy apply legal norms and issue departmental normative acts according to their competence (defined by Ukraine's current legislation): decisions, resolutions, instructions, directives, letters, and explanations. Rulemaking is one of the main functions of national security governance.

Relations in this area are regulated, in particular, through periodic updates of the National Security Strategy of Ukraine and sectoral doctrines, concepts, and programs, as well as through the process of planning and implementing specific practical measures to neutralize threats to national interests.

In general, the legal basis of national security is two-tiered. The first level is mandatory for all and provides for the formation of the national security system (the Constitution of Ukraine, laws and resolutions of the Verkhovna Rada of Ukraine, resolutions and orders of the Cabinet of Ministers of Ukraine, decrees and orders of the President of Ukraine, decisions of the National Security and Defence Council of Ukraine). At the second level, a departmental regulatory framework is formed, which details the functionality and tasks of each entity involved in ensuring national security.

The main objectives of the organizational and legal support of national security are to consolidate existing and form new relations legally, to regulate them effectively in the field of national security, and to prevent and eliminate situations that hinder the development of new progressive trends in the security sector.¹⁹

National Security Information and Public Administration Aspects

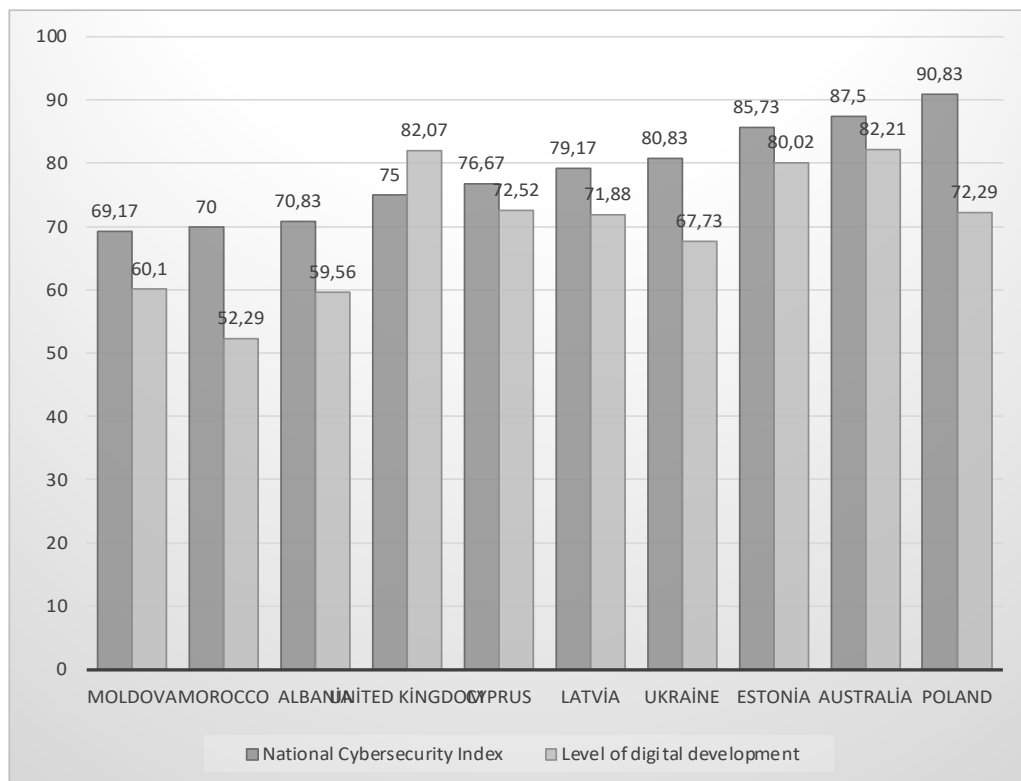
National security information and public administration aspects require a reliable and sustainable digital infrastructure. Cybersecurity in the public sector should be based on the principle of effectively implementing the functionality of the relevant public authorities, as well as on developing and implementing an effective strategy for developing the cybersecurity system and integrating modern tools for its implementation.

In particular, the National Cybersecurity Index (NCSI) demonstrates the state's

19) M. Albahar, "Cyber attacks and terrorism: A twenty-first century conundrum", *Science and engineering ethics*, Vol. 25, No. 4 (2019), p. 993-1006.

potential to mitigate cyber threats effectively. The corresponding ranking (Figure 1) shows the leaders in 2023.

Figure 1. NCSI ranking, 2023



Source: NCSI²⁰

The NCSI definition measures a country's ability to implement a practical cyber incident management strategy. The dynamics of this index allow us to track the progress of a country's digital development. As shown in Figure 1, Ukraine took fifth place in this ranking, representing the country's rapid digital development. The calculation of the Security Index is important for several reasons, including assessing the security climate, the state of policy planning and implementation, investment attraction, social stability and development, and international cooperation. The Index can serve as a basis for international cooperation and dialogue in the security sector, facilitating the exchange of experience and coordination of efforts to address common challenges. Analyzing Figure 1, it is worth noting the active progress of

20) NCSI (National Cyber Security Index) Cybersecurity Rating for 2023 (2024) – available at: <https://ncsi.ega.ee/country/ua/>

Poland and Estonia, which have recently joined the European single space. Ukraine has significant potential in this area.

Among the priority strategies for optimizing national security information support are the following:

- A systematic analysis of innovative threat identification technologies;
- Integrating the efforts of cyber defense specialists to perform security audits, implement technologies, and develop defense strategies;
- Implementation of strategic cyber resilience programs;
- Implementation of international security standards, expansion of international cooperation, exchange of experience, and joint training projects;
- Integration of innovative security, encryption, and multi-factor authentication technologies.

The capabilities of artificial intelligence and innovative technologies, as well as outsourcing and monitoring, are now actively used to create modern integrated information security systems (IIS). The basic principles of the IIS organization are systematic, flexible management, continuity of protection, openness of algorithms, and ease of use.²¹

The priority tasks that the IIS should successfully solve in the national security sector include:

- Effective management of access to confidential data;
- Protecting information data and monitoring the activities of system users;
- Ensuring the integrity of critical system resources;
- Management of protective equipment.

A progressive decision for Ukraine in this context was the ratification on 23 February 2023 of the Agreement on the country's participation in the EU's Digital Europe program,²² which offers an innovative format of opportunities for developing a digital society. Promising areas for developing the regulatory framework for the information security system in the public sector include the implementation of international norms on combating cybercrime and integrating innovative means of protecting digital infrastructure.

21) O. Zh. Skibun "Cybersecurity of electronic communications systems of public authorities of Ukraine", *Visnyk of the National Academy of Public Administration. Series "Public Administration"*, Vol. 1, No. 100 (2021), p. 30-39; I. Sopilko, "Information security and cybersecurity: a comparative legal aspect", *Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law"*, Vol. 2, No. 59 (2021), p. 110-115.

22) Agreement between Ukraine and the European Union on Ukraine's participation in the European Union's Digital Europe Programme (2021-2027) – available at. https://zakon.rada.gov.ua/laws/show/984_005-22#Text

Personnel and Public Administration Aspects in the Field of National Security

Personnel and public administration aspects in the field of national security include a wide range of intellectual, spiritual, cultural, and physical qualities of human capital that directly or indirectly influence the dynamics of the national security state. In light of digital transformation, human capital is implemented practically in operations and control based on the partial virtualization of processes.

Attention must be paid to the priority of the partnership concept, a system of public administration in which society and the state are equal participants (Table 1).

Table 1. The partnership concept in national security staffing

Principle	Specificity of the Impact
Democracy	Intensification of the significance of public influence on public administration processes in the field of national security
Priority of Decentralization	Decentralization of public administration processes, involvement of highly specialized personnel based on a centrifugal personnel policy
Strategic Approach	Prioritization of strategic goals of national security development, continuous improvement of human resource skills, ensuring compliance with current requirements
Complexity	The balance between state and public regulation of the sphere, regular updating of the goals of public administration processes in the field of national security
Adaptability and Flexibility	Provision for regular professional development of specialists, organization of training with the involvement of international practical experience, implementation of international competence standards

Source: Provided by the author(s).

Adherence to these principles implies developing and implementing state and regional programs for developing individual industries, segments, and sectors of the national security sphere based on publicity and open access to the public. The innovative strategy of public administration of national security is focused on the motivated interaction of society and the state to guarantee the national space's economic, political, and social security, using the maximum capabilities of modern technologies and digitalization.

In the future, the potential of public administration in the overall public administration paradigm is seen as promising. This will inevitably provoke new challenges and risks but will significantly intensify the effectiveness of national security policy.

Discussion

The belief that one of the most promising means of improving the national security system is the active use of public administration instruments is popular in the modern scientific field.²³ According to scientists, foreign experience convinces us of the crucial role of public authorities in coordinating the actions of administrative actors in national security. At the same time, the development and legislative consolidation of types of responsibility in the field of national security becomes a priority.

Some scholars consider the possibility of digitalizing a significant share of public administration processes in the security sector.²⁴ According to scientists, the main goal is the accumulation, protection, and optimal use of information data. E. Klijn and J. Koppenjan²⁵ emphasize that insufficient access to modern technologies and the unwillingness of responsible personnel to implement them in practice are the main factors limiting the potential of public administration in the field of national security. Considerable attention should be paid to developing human potential and continuous professional development to meet the requirements of the digital society.

D. Mandel and D. Irwin pay special attention to the need for practical interaction between governments, society, and businesses regarding democratic development and the implementation of national security principles. The authors argue that although intelligence organizations have incredible information-gathering technologies at their disposal, analysts transform raw data into assessments for managers who make final decisions on national security. Given this, the priority areas for strengthening the modern security environment are information, personnel, and proper legal and regulatory support.²⁶

Scientist El-Muhammady identifies specific prerequisites for national security, the availability of an appropriate resource base, and society's readiness for dynamic change. The researchers propose the integration of blockchain and artificial intelligence technologies to ensure information security, as well as transparency, efficiency, and accessibility of public administration processes. The researchers pay special attention to the need to optimize the institutional framework that will facilitate the integration

23) O. Akimov et al., "International experience of public administration in the field of national security", *J. Legal Ethical & Regul. Issues*, Vol. 23 (2020), p. 1; N. Leonenko, "Foreign experience of legal regulation of national security", *Bulletin of the National Centre for Civil Defence. Series "Public Administration"*, Vol. 1, No. 18 (2023).

24) A. Babuta et al., *Artificial intelligence and UK national security: policy considerations. Technical Report*. (RUSI, London, 2020); E. H. Klijn & J. F. Koppenjan, Public management and policy networks: Foundations of a network approach to governance, in *Making Policy Happen* (London, Routledge, 2020), p. 28-40.

25) E. H. Klijn & J. F. Koppenjan, "Public management and policy networks: Foundations of a network approach to governance", in *Making Policy Happen* (London, Routledge, 2020), p. 28-40.

26) D. Mandel, D. Irwin, "Uncertainty, Intelligence, and National Security Decisionmaking", *International Journal of Intelligence and CounterIntelligence*, Vol. 34, No. 3 (2021), p. 558-582.

of IT into security management processes.²⁷

Y. Li and Q. Liu analyze the specifics of the geographical dimension of cyber threats and their aspects of vulnerability. The scientists see the formation of effective bilateral cooperation between the public sector, business, and the public in the context of jointly combating cyber threats as a necessary requirement for national security.²⁸

In continuation, R. Lau et al. propose several methods for modeling threats in cybersecurity. The authors argue that the ability to resist intrusions can be significantly higher if more protection resources are invested in critical infrastructure.²⁹

Despite significant scientific developments, rethinking the functionality of information, human, and legal resources in national security against the background of crisis conditions of social development requires extended scientific research.

Conclusion

The study substantiates that the public management aspects of ensuring national security today are expressed in developing cybersecurity, human resources, and improved legal support. Considering global digitalization, combining the efforts of society, business, and public authorities makes it possible to formulate a strategy for transforming the national security system.

The analysis of the main problems, challenges, and achievements of the information transformation of the security sector in the context of digitalization shows that the sustainability of security largely depends on the level of implementation of digital innovations for risk management. It is established that the main methods of ensuring national security today are technical and digital innovations, in particular, artificial intelligence tools and blockchain technologies, analysis and monitoring of cyberattack technologies, cooperation with international institutions, as well as adequate regulatory support complementary to the requirements of the present and raising public and civil servants' awareness of digital security.

The article analyses the NCSI (National Cyber Security Index) cybersecurity rating and the level of digital development in several countries, including Ukraine. The specifics of creating modern integrated information security systems, which today involve artificial intelligence and innovative technologies, require upgrading the legal framework and rulemaking to ensure national security. In addition, high-quality

27) A. El-Muhammady, "Balancing national development, national security, and cybersecurity policy", In. *Routledge Companion to Global Cyber-Security Strategy* (2021).

28) Y. Li & Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", *Energy Reports*, Vol. 7 (2021), p. 8176-8186.

29) P. Lau et al., "A cybersecurity insurance model for power system reliability considering optimal defence resource allocation", *IEEE Transactions on Smart Grid*, Vol. 11, No. 5 (2020), p. 4403-4414.

human resources have a significant potential for maintaining an adequate level of national security.

Among the main directions of strategic development of the system of public management of security processes in the context of globalization are the integration of the principle of mutual responsibility of the individual, society, and the state, development of interaction and coordination of the state and non-state subsystems of national security, prompt information and coordination of actions of the national security forces; provision of the population with reliable information; introduction of positive international experience in organizing the activities of the system of national security.

Among the areas for further research on the topic under study, it is worth focusing on analyzing the potential of digital technologies to guarantee national stability, ensure the observance of citizens' rights, and increase investment opportunities.