National Security Management: Organizational, Legal, Informational and Human Resource Dimensions

Alina Pomaza-Ponomarenko [1], Dmytro Taraduda [2], Oleh Kravchuk [3], Svitlana Moroz [4], Olena Akhmedova [5], Stanislav Poroka [6]

[1] Scientific Department for State Security Problems, Training Research and Production Centre, National University of Civil Defense of Ukraine, 94 Chernyshevska Str., Kharkiv, 61023, Ukraine.
[2] Department of Emergency Situations Elimination, Institute of Postgraduate Education, Lviv State University of Life Safety, 35 Kleparivska Str., Lviv, 79007, Ukraine.
[3] Department of Criminal Law and Procedure, Leonid Yuzkov Khmelnytskyi University, 8 Heroiv Maidanu Str., Khmelnytskyi, 29013, Ukraine.
[4] Military Institute of Tank Troops, National Technical University "Kharkiv Polytechnic Institute", 2 Kyrpychova Str., 61002, Kharkiv, Ukraine
[5] Kyiv National University of Technologies and Design, 2 Mala Shyianovska Str., Kyiv 01011, Ukraine.
[6] National University of Civil Defense of Ukraine, 94 Chernyshevska Str., Kharkiv, 61023, Ukraine.

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: Enhanced security threats in wartime and post-crisis environments that require systemic resilience and the protection of national interests entail implementing national institutional, informational, legal, and human resources to their fullest capabilities. In so doing, it offers an unparalleled overview of the organizational, legal, informational, and human factors within public management that shape the performance of the national security system. This paper articulates and theorizes central principles for constructing a modern national security system featuring a hierarchy of national interests, multi-level state, sub-state, and non-state actor coordination, transparency, and attunement to global best practices. Utilizing NCSI as an empirical reference frame, the paper discusses the transformation of cybersecurity and digital preparedness capabilities among EU members for the period 2023–2025, displaying a longer-term view of increasing cyclicality of cyber resilience across the European security architecture. Strategic implications: the study suggests that the IIS's evolution must be based on a synergy of technological innovation, sound legal regulation, and competent human resources. The structure and processes of national security governance, therefore, need to be transformed into strategic decentralization, interinstitutional cooperation, and digital inclusion. The findings advance the theory and practice of the impact of digital transformation on national security governance mechanisms and provide conceptual premises for improving public management strategies in an age of globalization and technological convergence.

Keywords: authorities, civil protection, information security, legal support, national security, public administration.

Introduction

The directions of national security, on which the strategy of development should be built, are political, legal, financial, knowledge and information, techno-energetic, ecological, social, socio-psychological, religious, moral, educational, and military potential, and a system of complex stability. The successful implementation of this strategy is contingent upon the well-balanced operation of national government agencies. These agencies must consistently collaborate with other stakeholders within and beyond their respective spheres to identify and foresee, as well as to address, both current and future threats that could potentially disrupt the national landscape due to domestic and foreign influences. The national security strategy is meant to contribute to a foundation for the free play of national interests and to be a source of adequate protection against risks and threats sourced in the contemporary environment. Thus, this ideal is achieved by having "consistent" unfolded layers–informative, organizational, legal, and personal petroleum–all of which contribute an indispensable piece to the system's ability to sustain/exploit. So

with global geopolitical upheaval, technological interdependence, and changing models of security, the NSS must be reiterated and re-examined.

Literature Review

The transformation in national security knowledge that is beginning to emerge from recent research indicates that managing security at the national level is not just a matter of having the right national-level institutional arrangements; it is a matter of leveraging the human-based, digitally based, and legally based resources that can address complex threats in a world of shifting political and technological parameters.

Organizational Dimension

Ciekanowski et al. [1] found that the quality of performance, as well as that of survival, of security agencies is affected by the organizational level; the element of human resources is paramount in ensuring strategic coherence and the level of performance. Similar to systemic organizational conceptions of national security, Kotliarov [2] discusses aspects of institutional function coordination, as well as decision-making procedures, that bring public and private agents into accord. Kallunki [3] elaborates on this notion to assert that the resilience of national security systems, in periods of sociocultural flux, is defined by institutional collaboration through adaptive governance and the vacuum of continuous professional development via organizational arrangements. To conclude, these studies underline that organizational coherence and managerial flexibility are what make it possible to address the hybrid threats and the threat of asymmetric warfare.

Legal Dimension

The legal aspect is one of the cornerstones on which national security is established. Alguliyev [4], Viter and Rudenko [5], and several other scientists believe that a complex legal regulation of national security allows us to distinguish states, public and informational security on different levels, and have a stable policy structure of the corresponding subject of power. This legal basis makes it possible for national security doctrines to be formulated and for institutional powers to be delineated. Concerning national security, Ortynskyi [6] also insists that the contemporary national security administration necessitates the development of public-private-partnership-based legal tools, more concretely in the field of cybersecurity and information protection. Tsybulnyk [7] adds to this view by keeping with the state security sector's legal and institutional features and clarifying the need to meld informational and juridical safeguards in maintaining sovereignty. Amoo et al. [8] emphasize that effective national security management is impossible without harmonizing cybersecurity and personal data regulation, where the General Data Protection Regulation (GDPR) is a key tool for balancing information protection and national interests. Babikian [9] believes that modern national security management should integrate cyber law mechanisms to adapt to new digital threats and transnational challenges in cyberspace.

Informational Dimension

One of the earliest to point out that information security is a management problem rather than a technology problem and needs to be embedded within business processes and human systems, well before the media hype on this particular angle in the 2000s, was Michael [10]. Dragomir [11] also builds upon this thesis by arguing that information systems are transforming national security strategies through increased interoperability, situational awareness, and command decision-making. Ortynskyi [6] serves as an example: Both Ortynskyi [6] and Tsybulnyk [7] reveal how robust information governance can protect national information resources from cyber and cognitive attacks. Kallunki [3] examines national security management through the prism of societal information resilience, emphasizing the need for collective preparedness among citizens as a component of comprehensive security. Mousavi and Gu [12] argue that effective communication by government agencies on social media is critical for maintaining social stability and compliance with safety regulations during crises.

Human Resource Dimension

Mazilu [13] considers that the HR management system modernization, especially in terms of digitalization and development of leadership, leads to the institution becoming more adaptable as well as to a reduction of long-term running costs. Ciekanowski et al. [1] also maintain that human resources underpin the organizational security architecture through selection, development, and motivation processes that align persons with strategic ends. Arifkhodzhaieva [14] holds the view that for the system of national security to overcome the human element, participatory training, and leadership enhancement are crucial. Overall, investing in human capital is a strategic buffer that supports the sustainability and flexibility of security organizations.

Integrated Perspectives and Research Gaps

Emerging studies [2,11,15,16] signal converging calls for a unifying and trans-dimensional national security management framework. It is worth mentioning that, interestingly, Kobko et al. [15] view regulatory, organizational, informational, and human resource aspects of response to threats (in particular in the process of armed aggression). Scholars contend that jural, informational, and human components of security governance remain underexplored empirically vis-à-vis the effects of digital transformation upon each of these. Moreover, the developing relationship between organizational culture, legal flexibility, and cyber resilience has not been explored fully in the literature.

A review of the literature reveals that national security management encompasses the aspects of organizational effectiveness, quality of law, quality of information, and enhancement of human resources. Although prior literature clearly lays the foundation for conceptual and normative frameworks, more empirical research is warranted to develop integrative models that articulate interactive effects among these constructs. These kinds of models may help explain how states can sustain security capacity in an era of uncertainty, complex digital interdependence, and hybrid threats.

The purpose of this work is to conduct a deep analytical analysis of the public administration organization, legal, information, and human resources aspects in providing national security in the sphere of its extreme digital transformation. Specific focus is placed on determining the relations between institutional capacity, level of maturity of digital infrastructure, and public-governance mechanisms that adapt to guarantee cyber-resilience and strategic national-interest protection.

Materials and Methods

Both the empirical part and the theoretical framework of the study are based on scientific literature, policy reports, and data from global indices on cybersecurity and digital development. These include the National Cybersecurity Index [17], the Global Cybersecurity Index (GCI), the ICT Development Index (ICTDI), and the Network Readiness Index (NRI). In addition, to provide a comparative and integrative analytical framework for the study, documents from scientific and professional conferences and documents related to EU digital policy, as well as the national regulatory approaches taken by Ukraine and the EU member states, were also consulted.

A repertoire of interrelated research methods was employed to facilitate multi-layered and non-biased examination. The research used systemic and structural-functional methods of analysis, enabling the exposure of relationships among institutional, technological, and legal components of national security. The technique of comparative analysis was used to evaluate the processes of development of regulatory and managerial tools in Ukraine in comparison with the best practices of the EU and international standards on cybersecurity.

Analytical and synthetic thinking were employed together to merge theoretical with empirical knowledge. By analysis, to explore determinants of effective national security governance; by synthesis, to conceptualize those determinants in a systems model of public administration.

Theoretical statements regarding human capital, information management, and legal adaptation about the nature of national security in digitalization were developed using the principles of abstraction.

At the empirical level, the analysis entailed the gathering of basic descriptive statistics on indicators of cybersecurity and digital readiness for EU member states, ranging over the period 2023–2025, drawing on official NCSI [17] data. Data analysis and visualization were performed using the JASP software, allowing us to analyze the success of the digital transformation protocols, as well as their effect on the indicators of data protection and resilience.

This integrated approach ensured scientific soundness and reproducibility as well as cross-national comparability of the results, thereby strengthening the analytical power of deductions concerning the development of a digitally sustainable national security system.

Results

The functions of state security can be considered a complex, multi-layered system of related components working to predict, prevent, and counteract both present and future threats to national sovereignty and sustainable development [18]. In modern times, the concept of national security is not to be seen from the point of military or defense organization alone but rather as a systemic complexity involving organizational, legal, informational, and human-related elements [1,2,4,11,19].

The development of a coherent national security policy framework must be grounded on a few principles that would guarantee a convergence between domestic and foreign policy, institutional adaptiveness, and public support. Here

are some of those principles: the dominance of the national interest principle; the national security of consensual principle; the principle of coordination and cooperation; the principle of transparency and trustworthiness; the principle of managerial accountability and proportionality; the principle of systemic balancing; the principle of 'openness to international experience'.

Readiness for combat, mobility, coordination, situation awareness, and institutional durability are also indicators of a well-developed and sustainable security system [20]. Yet, in the age of digitalization and hybrid threats, cyber resilience, data integrity and adaptability of human resources are considered useful criteria to assess the performance of a national security system [11,13,21]. As a result, contemporary national security governance signifies a dynamic, knowledge-centric system that harmonizes self-governance, legal operation, information transparency, and human development, each as an integral element of sustaining the state amidst global uncertainty.

The public administration in the national security sphere is determined by the institutional and legal baseline, and that sets the functioning conditions for the whole system. They sit within a multi-tiered system of governance involving constitutional norms, legislative acts, and sectoral regulations. These tools carve out the power, the responsibility, and the accountability of state and non-state actors [7]. In Ukraine, the system is reflected in the Constitution of Ukraine and the legislation On National Security of Ukraine and On the Fundamentals of Domestic and Foreign Policy and other aggregates of legal acts that all contribute to aligning the system with democratic-governance and the rule of law. Under this conceptual umbrella, national security institutions–ministries, defense agencies, intelligence bodies, and specialized services – do not simply implement statutory provisions but also formulate sectoral norms through a series of internal rulings, instructions, and departmental regulations [22].

These normative instruments transform strategic national security policy goals into action and keep its legal malleability in the medium of continuous geopolitical and technological transition [15]. The process of rulemaking thus becomes an essential function of national security management, translating strategic priorities into legally binding mechanisms of coordination and oversight.

National security governance within a government often involves a two-tier system. The first, constitutional-legislative, layer consists of general obligatory normative acts – the Constitution, Laws, Decrees of the president, resolutions of the Verkhovna Rada and rulings of the NSDCU which establish the general principles of organization of the national security system. The second (ministerial executive) level is made up of sector-specific internal policies, doctrines and arrangements, which outline, within them, the public authority's domain, and the mode in which it is exercised, the minimum procedural standards which those public authorities applying for cooperation in the provision of security must meet [13]. Functional differentiation: "Acting out of their competence," Each level of governance can therefore pursue its own segment of the security policy with sufficient normative clarity and administrative ability.

The complex of organizational-legal provision is oriented to systematization and unification of regulatory relations in the sphere of safety. It seeks to create a legal infrastructure enhancing innovation and collaboration and facilitating crisis response and adaptive policy development while dismantling institutional barriers to adaptive policy development [2,23]. In accordance with the European and NATO standards, Ukraine's reform activities in the legal and organizational sphere also include an update of the National Security Strategy regularly and the introduction of specialized doctrines and focused state programs. These key instruments contribute to the adaptation of the security policy to evolving hybrid threats, cyber threats, and the growing complexity of the international environment [6,14].

Yet the growth of the cyber aspect of national security, on the other hand, must be paralleled by unremitting surveillance of the state's digital resilience–not simply by legal and bureaucratic tinkering. The trends of the National Cyber Security Index (NCSI) in the EU members, 2023–2025 (see Figure 1), reflect a gradual improvement in the level of national cyber resilience and serve as evidence of the strengthening of strategic protective actions in the digital domain.

Next page

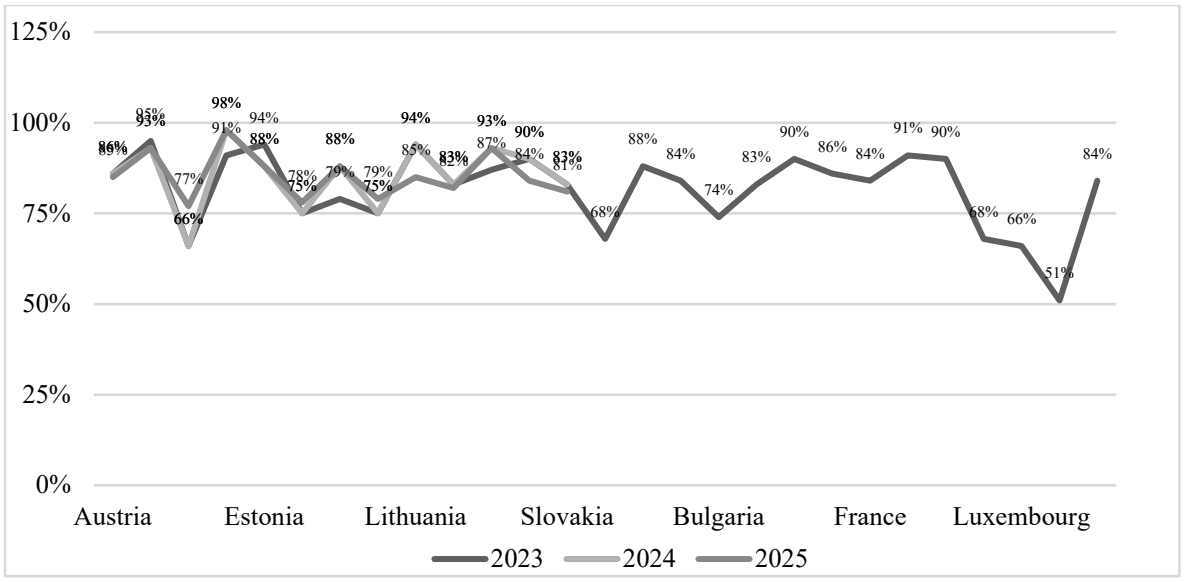

Figure 1. Dynamics of the National Cyber Security Index (NCSI) in EU member states during 2023-2025
Source: NCSI [17]

As can be seen from the presented data, most of the European Union member states demonstrate stable positive dynamics, reflecting the active implementation of national digital security strategies and the growth of the level of interstate coordination in the field of cyber defense. Significantly, Estonia, Poland, Finland and the Netherlands maintain high positions in the ranking, which systematically invest in the development of digital infrastructure, personnel training and the implementation of artificial intelligence in cyber incident management. For Ukraine, the positive dynamics within the European cyberspace indicates the effectiveness of current reforms, in particular the implementation of the National Cyber Security Strategy [24], active participation in the Digital Europe program, as well as gradual integration into the European cyber defense system. At the same time, maintaining sustainable results requires building a national cyber resilience infrastructure, which involves developing institutional capacity, technological sovereignty, and training highly qualified specialists [25,26].

An in-depth analysis of the dynamics of the NCSI requires a comparative consideration of the relationships between different indicators of digital readiness of EU countries. To this end, descriptive statistics were conducted on the original data set for 2023–2025, which summarizes the main parameters of four key indicators: NCSI (National Cyber Security Index), GCI (Global Cybersecurity Index), ICTDI (ICT Development Index), and NRI (Networked Readiness Index).

These indices characterize not only the level of technical security, but also the depth of digital integration of state institutions, the degree of institutional maturity of the cyber risk management system, and the readiness of national economies to digital challenges. To conduct the relevant analysis, descriptive statistics of the original data set (Appendix A) were compiled, which are presented in Table 1.

Next page

Table. 1. Descriptive statistics of cybersecurity and digital readiness indicators of EU countries during 2023-2025

Descriptive Statistics												
Descriptive Statistics												
Period	*2023*				*2024*				*2025*			
Indicators	NCSI	GCI	ICTDI	NRI	NCSI	GCI	ICTDI	NRI	NCSI	GCI	ICTDI	NRI
Valid	27	27	27	27	13	13	13	13	13	13	13	13
Missing	0	0	0	0	14	14	14	14	14	14	14	14
Median	84.000	94.000	78.000	5.000	88.000	95.000	80.000	5.000	85.000	94.000	86.000	63.000
Mean	81.667	91.296	76.259	4.667	85.538	94.154	80.000	27.538	85.462	93.846	87.462	63.000
Std. Deviation	10.655	8.708	6.087	0.620	9.070	4.259	7.360	30.223	6.372	5.064	5.348	5.148
Minimum	51.000	67.000	65.000	4.000	66.000	86.000	71.000	4.000	77.000	83.000	80.000	55.000
Maximum	95.000	100.000	87.000	6.000	98.000	100.000	97.000	68.000	98.000	100.000	97.000	74.000

Source: compiled by the author
Note: NCSI – National Cyber Security Index; GCI – Global Cybersecurity Index; ICTDI – ICT Development Index; NRI – Networked Readiness Index

The statistical feature analysis indicates that all indicators' mean value of digital security and readiness had an upward tendency in the study period. The NCSI mean value increased from 81.67 to 85.46, which validates an enhancement of the cyber defense capabilities of the EU member states. Positive results can also be seen in the Global Cybersecurity Index (GCI), reflecting the fortification of the institutional setting, especially in areas related to formulating strategies, regulations, and the establishment of national CERT centers. The growth of both the ICT Development Index and the Networked Readiness Index in 2025 shows that there is a holistic development of digital infrastructure, especially in the aspect of cloud technology development and utilization of AI in the domain of cyber defense. Meanwhile, a reduction of dispersion (a decrease of standard deviation) implies that two countries' level of digital readiness is becoming more alike, i.e., the convergence of standards and the harmonization of the European cyberspace are gradually taking place. In other words, national cybersecurity policies seem to be converging, at least to some extent, within the context of the EU Cyber Resilience Act instrument. Hence, the conducted analysis points towards an

equalizing effect of digital convergence among EU member states, dictated by the coordination mechanisms, pan-European training schemes, and common standards in the area of cybersecurity.

In the ever-changing national security landscape, information support systems have become essential strategic assets. Their evolution is based on a number of interdependent pathways. Firstly, a systematic research on the new technologies for threat detection is needed since traditional methods for detection are inadequate for the new forms of war, especially modern hybrid forms and cyber forms of war [27]. Second, the convergence of cyber-defense specialists into integrated organizations that conduct audits, leverage emerging technologies and formulate coordinated defensive tactics is emerging as a consolidated system of collective defense [28]. Third, the realization of strategic cyber resilience enables states to withstand, and to recover from, devastating cyber attacks by means of resilience-centric designs and adaptive infrastructures [6]. Fourth, a deepened commitment to international security norms, enhanced cross-border collaboration, and the sharing of best practices and training contributes to the integration of national security agendas into a broader regime of global governance [29]. And, in an era of advancing technologies – portable computing, smart grid, cloud computing, predictive analytics, advanced encryption methods, multi-factor authentication, AI-based monitoring, and flexible outsourcing models – features coalesce into integrated, adaptive and digitally mature information security systems [25,30].

The utilization of IIS enabled by AI, big data analytics, and real-time monitoring is the basis of these methodologies. The organizational form of such a system follows from systemicity, flexible governance, protection continuity, algorithmic transparency, and user-friendliness [26,31]. These design features are in line with the general agreement from the literature that information security needs to go beyond technological controls and encompass governance, organizations, and legal constructs [28].

The operational priorities for an IIS in the national-security context can be stated as (i) managing and controlling access to classified or sensitive information; (ii) protecting information and tracking users inside the system; (iii) assuring the quality of system-sensitive resources; and (iv) administrating and using protective infrastructure and hardware.

Ukraine's strategic forward movement in this field of action is demonstrated by its accession to the Digital Europe Programme on 23 February 2023, which opens new avenues for the development of digital society and brings domestic undertakings closer to EU digital-infrastructure goals. Increasing attention is being paid to regulatory structures that embed international standards for combating cybercrime, the introduction of new protections for digital infrastructure, and the development of capacity for human capital resilience [32].

From the human resource and public administration viewpoints, the provision of national security personnel has evolved from a simple number of bodies to that of utilizing an array of human capital (intellectual, cultural, digital, and physical) to shape system resilience and system adaptability in the era of digital. Human capital realization is increasingly taking place through (partial) virtualization of operational and control procedures. One core component of governance models that is being developed in the literature is the notion of the partnership model, which imagines society and the state as co-equal partners within a communal public-administration system.

Next page

Table 2. The Partnership Concept in National Security Staffing

Principle	Specificity of Impact	Functional Dimension	Expected Strategic Outcomes
Democratic Governance	Expands the influence of civil society on strategic decisions in the national security domain through participatory mechanisms and deliberative policy models.	Political-administrative	Strengthening of public trust, increased transparency, and legitimacy of national security institutions.
Priority of Decentralisation	Delegates part of decision-making authority to regional and sectoral levels, ensuring the inclusion of local expert communities and rapid adaptation to situational challenges.	Organisational territorial	Formation of adaptive regional security clusters and improved operational responsiveness.
Strategic Approach	Focuses on long-term development trajectories of the human-resource potential, competency planning, and knowledge continuity in security governance.	Strategic-managerial	Sustainable evolution of personnel capacity aligned with future-oriented national security priorities.
Complexity and Systemicity	Recognises the interdependence of political, legal, economic, technological, and socio-cultural factors shaping the resilience of the national-security system.	Systemic-integrative	Enhanced coherence among national, sectoral and institutional security subsystems.
Adaptability and Flexibility	Provides for dynamic updating of professional standards, development of digital competencies, and operational flexibility in crisis conditions.	Human-capital	Formation of agile and cross-functional professional teams with rapid learning capabilities.
Public-Private Partnership (PPP)	Encourages collaboration between state institutions and private digital, technological, and analytical sectors for shared implementation of cyber-resilience projects.	Economic-innovative	Expansion of innovation diffusion and co-financing models in critical-infrastructure protection.
Ethical Responsibility and Accountability	Establishes moral and legal responsibility of decision-makers for management outcomes and adherence to democratic values and human rights.	Legal-ethical	Institutionalisation of accountability mechanisms and minimisation of abuse or corruption risks.
Transparency and Openness of Information	Ensures access to verified data, public monitoring of national-security programmes, and the prevention of information asymmetry.	Information-communicative	Improvement of information trust, decrease in disinformation impact, and higher resilience to hybrid threats.
Integration of International Experience	Facilitates the adaptation of international best practices, standards, and digital-security models to national conditions.	Cross-border cooperation	Harmonisation of Ukraine's security architecture with EU and NATO frameworks.

Continuous Professional Development	Institutionalises the lifelong learning model, ensuring the regular upgrading of skills in cybersecurity, strategic communication, and digital governance.	Educational-professional	Formation of a knowledge-intensive and technologically proficient workforce.
Innovative Competence Management	Introduces digital HRM instruments (AI-based analytics, predictive personnel modelling, adaptive learning systems) to optimise staffing in security institutions.	Digital-managerial	Increased efficiency of personnel allocation and improved forecasting of human-capital needs.
Resilience and Crisis Preparedness	Prioritises proactive training in emergency management, resilience planning, and stress resistance of personnel.	Socio-psychological	Strengthened institutional stability and minimised performance decline under stress or threat.
Intersectoral and Interagency Coordination	Enhances the interaction of ministries, regional administrations, and non-governmental structures in joint risk-management networks.	Governance-network	Formation of a synergistic governance ecosystem that prevents duplication and accelerates decision-making.
Digital Ethics and Data Sovereignty	Regulates the use of personal and classified data, AI systems, and algorithmic decision-making to prevent violations of information sovereignty.	Normative-technological	Legal protection of digital assets and balance between openness and confidentiality.
Motivation and Value-Based Leadership	Establishes leadership principles built on patriotism, civic responsibility, and intrinsic motivation for safeguarding the state.	Socio-cultural	Increased engagement, morale, and collective responsibility among personnel.

Source: compiled by the author based on Skibun [26], Sopilko [31], Rass et al. [20], Nowicka et al. [28], Benzar et al. [25], Melnychenko et al. [32], Pomaza-Ponomarenko et al. [33]

Following these principles requires the creation and execution of state- and region-level solutions focused on a discrete portion of the national security space (industries, domains, and subsystems) predicated on transparency and public access. The changing model of public administration in national security increasingly appears as a stable but motivated interaction between society and the state based on the utilization of modern technologies and digitalization to ensure economic, political, and social stability. However, the future potential of its paradigms on public administration in the overall governance network appears considerable: although new challenges and risks will materialize, the transition to digitally enabled, partnership-oriented national security policy appears likely to provide a substantial boost to effectiveness and resilience.

Discussion

The empirical and theoretical results obtained in this paper corroborate and extend the existing literature on the polycentric nature of NISM, while they provide novel evidence on cyber resilience, digital readiness, and human capital adaptability as leading enablers for systemic vitality. The ensuing discussion is a synthesis of these findings in the light of the theoretical debates identified at the outset and in relation to the unique contributions derived from the empirical and conceptual integration.

Convergence of Organisational and Legal Dimensions

The results confirm the conceptual argument presented by Ciekanowski et al. [1] and Kotliarov [2] that the governance of national security is organizational and depends on the stability and flexibility of the organization itself. The two-level configuration of Ukraine's security regulation observed herein–which embraces constitutional-legislative and departmental-executive levels–actualizes the systemic differentiation, i.e., it has the function of turning strategic goals into concrete and binding solutions [7]. The implications of this research are, however, far-reaching in that legal and organizational systems are now shown to be progressively evolving. In essence, the administrative capacity of institutional and organizational reform is contingent upon a nebulous and open legal system, which in turn is dependent on the co-evolution of the success of legal evolution.

Integration of Informational Resilience and Cyber Readiness

The result obtained in the study provides conceptual and empirical justification for the claims made in Dragomir [11] and Ortynsky [6], where information systems were the management of national security. The increase in the average value of the NCSI and GCI indicates that the systemic form of adequacy–among the results of the analysis–is formulated as a principle that can be interpreted as the fit for purpose of the digital infrastructure, legal instruments, and the sustainability of the management actions for cyber defense management. It is clear that these empirical results contribute to bridging the conceptual gap identified by Kobko et al. [15] regarding the theoretical rationale for including DT in all safety management models.

Human Capital and Partnership-Based Governance

In line with Mazilu [13] and Arifkhodzhaieva [14], the study demonstrates that human capital is both a source and a vector of national security. Still, the integration of the partnership concept into the domain of national security staffing creates a new paradigm that renders viable the exploitation of human capital in democratic governance, decentralization, and digital competence building. This theoretical approach adds to the one proposed by Ciekanowski et al. [1], considering sociocultural, ethical, and technological facets of HRM in the context of personnel selection and motivation. In line with these results, our findings are in agreement with those of Benzar et al. [25] and Nowicka et al. [28], which identify AI and predictive analytics as enablers for personnel optimization.

Following the analysis of the results from the categories concerning organizational legal, information, and human resources, a national security management-centric holistic cyber-governance paradigm can be observed. Differing from previous views [2,10], which at times considered these components in isolation, this study demonstrates their ongoing co-constitution. In particular, the deployment of AI in Information and Security Systems (ISS) results in a cybernetic feedback loop–a dynamic, self-regulating relationship among the information flow, decision making, and risk analysis. This serves to extend the "skilled-securer knowledge system" metaphor as discussed by Skibun [26] but lends positive proof of AI-derived surveillance and digital values based ethics as a concept on the level of a holistic principles. This leads to a theoretical suggestion, which I call the integrated cyber-resilience model (ICRM), built on the three following assumptions: (1) on the macro-level: as the environment evolves, organizational adaptability and legal flexibility need to co-evolve; (2) on the meso-level: informational resilience, and not technological autonomy, derives from synchronized governance; and (3) on the micro-level: advancing human capital is the very foundation of cyber resilience and institutional sustainability.

Conclusion

Theoretical, structural, and technological elements of the public administration system in relation to the national security system in the context of the global digital environment are clearly verified by the study. The results indicate that the triadic society-business-government is the systemic resilience tipping point. Such cooperation allows us to coordinate our efforts in transforming the national security system into an adaptive, innovation-driven system that anticipates and disrupts complex hybrid attacks. Analyzing the NCSI, among other relevant measures of digital development, for EU member states and Ukraine revealed consistent advances in cyber resilience. This is the confluence of two processes: an increasing rate of technological inventiveness and a new set of rules, norms, and expectations for development and use. These findings could be related to the whole-of-government model for national security, in which security is identified as an emergent, knowledge-centric, and digitally enabled system. Future research should focus on assessing how technological innovation, social trust, and governance efficiency interact and whether digital technology can be leveraged to strengthen the protection of citizens' rights, improve the country's investment climate, and contribute to country stability.

References

1. Ciekanowski, Z., Nowicka, J., Żurawski, S., & Mikosik, P. (2023). Human Resources in Organizational Security Management. *European Research Studies Journal*, *26*(4), 802–812 https://doi.org/10.35808/ersj/3328
2. Kotliarov, V. O. (2023). The concept of strategic management national security. *Ukrainian Journal of Applied Economics and Technology*, *8*(1), 159–165. https://doi.org/10.36887/2415-8453-2023-1-23
3. Kallunki, V. (2024). Information Resilience as a Relational Infrastructure of Society: Collective Preparedness from the Standpoint of Citizens. In P. Uusikylä, H. Jalonen, A. Jokipii (Eds.), *Information Resilience and Comprehensive Security: Challenges and Complexities in Wicked Environments* (pp. 259–281). Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-66196-9_12
4. Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. S., & Aliguliyev, R. M. (2021). Information security as a national security component. *Information Security Journal: A Global Perspective*, *30*(1), 1–18. https://doi.org/10.1080/19393555.2020.1795323
5. Viter, D., & Rudenko, O. (2025). National security in the multi-domain environment: public administration issues. *Public Administration and Law Review*, (1(21)), 40–49. https://doi.org/10.36690/2674-5216-2025-1-40-49
6. Ortynskyi, V. (2025). Information Security in the Context of National Security: Legal Mechanisms for Protecting State Information Resources. *Veritas: Legal and Psychological-Pedagogical Research*, *1*(1), 1–9. https://doi.org/10.23939/veritas2025.01.001
7. Tsybulnyk, N. (2024). A Modern View on the Issue of Administrative Responsibility for State Security. *Baltic Journal of Legal and Social Sciences*, (4), 12-17. https://doi.org/10.30525/2592-8813-2023-4-2
8. Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), 1338–1347. https://doi.org/10.30574/ijsra.2024.11.1.0220
9. Babikian, J. (2023). Navigating legal frontiers: exploring emerging issues in cyber law. *Revista Espanola de Documentacion Cientifica*, *17*(2), 95–109. https://doi.org/10.13140/RG.2.2.20264.55048
10. Michael, K. (2008). *Social and Organizational Aspects of Information Security Management*. University of Wollongong. https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1598&context=infopapers
11. Dragomir, F.-L. (2025). How Information Systems Are Reshaping National Security Strategies. *Romanian Military Thinking*, (1), 174–189. https://doi.org/10.55535/rmt.2025.1.10
12. Mousavi, R., & Gu, B. (2024). Resilience messaging: The effect of governors' social media communications on community compliance during a public health crisis. *Information Systems Research*, *35*(2), 505–527. https://doi.org/10.1287/isre.2021.0599
13. Mazilu, E.-A. (2023). The modernization of the human resources management system as a determining factor of national security. *Bulletin of "Carol I" National Defense University*, *12*(3), 137–147. https://doi.org/10.53477/2284-9378-23-38
14. Arifkhodzhaieva, T. (2024). The management methods in the sphere of state security in conditions of social transformation. *Visegrad Journal on Human Rights*, *4*, 5–11. https://doi.org/10.61345/1339-7915.2024.4.1
15. Kobko, Y., Martovytska, O., Burlakov, S., Nazymko, O., & Hanenko, I. (2024). Modern Threats to The National Security of the State and Ways to Overcome Them: Reassessment of Views in The Context of Armed Aggression. *International Journal of Religion*, *5*(5), 632–640 https://doi.org/10.61707/7r6jp921
16. Quan, J., Duan, Y., & Fu, Q. (2025). Enhancing national security: a multidimensional situational awareness model for emerging economic crime prevention. *International Journal of Information Security*, *24*(6), 1–24. https://doi.org/10.1007/s10207-025-01136-7
17. NCSI (2024). Cybersecurity Rating for 2023. *National Cyber Security Index*. https://ncsi.ega.ee/country/ua/
18. Ige, A. B., Kupa, E., & Ilori, O. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Adv. Res. Rev*, *19*(3), 344-360. https://doi.org/10.30574/gscarr.2024.19.3.0236
19. Kurnia, R. R., Saputro, G. E., & Murtiana, S. (2023). Management of human resources in national defense depend on defense economics point of view. *International Journal on Social Science, Economics and Art*, *13*(1), 1–11. https://doi.org/10.35335/ijosea.v13i1.201

20. Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). *Cyber-Security in Critical Infrastructures.* Cham: Springer. https://doi.org/10.1007/978-3-030-46908-5
21. Pomaza-Ponomarenko, A., Hren, L., Durman, O., Bondarchuk, N., & Vorobets, V. (2020). Management mechanisms in the context of digitalization of all spheres of society. *Revista San Gregorio*, 42. http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/issue/view/RSAN42/showToc
22. Albahar, M. (2019). Cyber attacks and terrorism: A twenty-first century conundrum. *Science and engineering ethics*, *25(*4), 993–1006. https://doi.org/10.1007/s11948-016-9864-0
23. Pomaza-Ponomarenko, A., Taraduda, D., Leonenko, N., Poroka, S., & Sukhachov, M. (2024). Ensuring the safety of citizens in times of war: Aspects of the organisation of civil defence. *AD ALTA: Journal of Interdisciplinary Research*, 14(1), 216–220. https://www.magnanimitas.cz/ADALTA/140139/papers/K_10.pdf
24. ONCD (2023). The National Cybersecurity Strategy. *The White House.* https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy
25. Benzar, A., Kovalenko, Y. O., Taranenko, A., Balynska, O., & Balynskyi, I. (2025). Organizational Context of Security Management: Implications for Information Systems. *Management:(Montevideo)*, *3*, 250–250. https://doi.org/10.62486/agma2025250
26. Skibun, O. Zh. (2021). Cybersecurity of electronic communications systems of public authorities of Ukraine. *Visnyk of the National Academy of Public Administration. Series "Public Administration"*, 1(100), 30–39.
27. Semenenko, O., Nozdrachov, O., Dobrovolskyi, U., Kliat, Y., & Koverga, V. (2025). Assessment of Legal Challenges and Solutions to Cyber Threats in Hybrid Warfare. *Democracy and Security*, 1–21. https://doi.org/10.1080/17419166.2025.2525758
28. Nowicka, J., Ciekanowski, Z., & Milewska, A. (2024). Information security management as the basis for the functioning of an organization. *European Research Studies Journal, 27*(3), 128–141. https://doi.org/10.35808/ersj/3427
29. Golunov, S., & Bitabar, A. (2025). Overview of Global Cross-Border Cooperation Experience. In *Bridging Borders: Central Asian Cross-Border Cooperation in a Comparative Global Perspective* (pp. 7–70). Cham: Springer. https://doi.org/10.1007/978-3-031-84253-5_2
30. Ahmed, F. (2024). Cybersecurity policy frameworks for AI in government: Balancing national security and privacy concerns. *International Journal of Multidisciplinary on Science and Management*, *1*(4), 43–53. https://doi.org/10.71141/30485037/V1I4P107
31. Sopilko, I. (2021). Information security and cybersecurity: a comparative legal aspect. *Scientific Works of Kyiv Aviation Institute. Series Law Journal "Air and Space Law", 2*(59), 110–115. https://doi.org/10.18372/2307-9061.59.15603
32. Melnychenko, B., Tsebenko, S., Khomyshyn, I., Sirant, M., & Yesimov, S. (2024). Organizational and legal principles of information security of enterprises in the conditions of martial law in Ukraine. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, *1*, 167–174. https://doi.org/10.33271/nvngu/2024-1/167
33. Pomaza-Ponomarenko, A., Kravchuk, O., Hubenko, I., & Taraduda, D. (2024). Managing emergencies: Utilising historical insights for strategic enhancement. *AD ALTA: Journal of Interdisciplinary Research*, 14(2), 135–139. https://www.magnanimitas.cz/ADALTA/140142/papers/A_26.pdf

Appendix A

Country	National Cyber Security Index (NCSI)			Global Cybersecurity Index (GCI)			ICT Development Index (ICTDI)			Networked Readiness Index (NRI)		
	2023	2024	2025	2023	2024	2025	2023	2024	2025	2023	2024	2025
Austria	86%	86%	85%	94%	94%	89%	80%	80%	91%	5%	5%	66%
Belgium	95%	93%	93%	96%	97%	97%	78%	81%	81%	5%	66%	66%
Bulgaria	74%	-	-	67%	-	-	69%	-	-	4%	-	-
Croatia	83%	-	-	93%	-	-	72%	-	-	4%	-	-
Cyprus	66%	66%	77%	89%	89%	97%	78%	78%	86%	4%	4%	57%
Czech Republic	91%	98%	98%	74%	88%	88%	72%	82%	82%	5%	63%	63%
Denmark	84%	-	-	93%	-	-	87%	-	-	5%	-	-
Estonia	94%	88%	88%	100%	95%	95%	81%	97%	97%	5%	68%	68%
Finland	86%	-	-	96%	-	-	79%	-	-	5%	-	-
France	84%	-	-	98%	-	-	82%	-	-	5%	-	-
Germany	91%	-	-	97%	-	-	84%	-	-	5%	-	-
Greece	90%	-	-	94%	-	-	72%	-	-	4%	-	-
Hungary	68%	-	-	91%	-	-	69%	-	-	4%	-	-
Ireland	75%	75%	78%	86%	86%	91%	80%	80%	91%	5%	5%	66%
Italy	79%	88%	88%	96%	100%	100%	70%	84%	84%	4%	64%	64%
Latvia	75%	75%	79%	97%	97%	83%	73%	73%	89%	4%	4%	58%
Lithuania	94%	94%	85%	98%	98%	93%	72%	72%	91%	4%	4%	60%
Luxembourg	66%	-	-	97%	-	-	85%	-	-	5%	-	-
Malta	51%	-	-	84%	-	-	79%	-	-	5%	-	-
Netherlands	83%	83%	82%	97%	97%	99%	85%	85%	95%	6%	6%	74%
Poland	87%	93%	93%	94%	94%	94%	69%	86%	86%	4%	60%	60%
Portugal	90%	90%	84%	97%	97%	100%	71%	71%	84%	5%	5%	62%
Romania	90%	-	-	76%	-	-	65%	-	-	4%	-	-
Slovakia	83%	83%	81%	92%	92%	94%	71%	71%	80%	4%	4%	55%
Slovenia	68%	-	-	75%	-	-	74%	-	-	5%	-	-
Spain	88%	-	-	99%	-	-	78%	-	-	5%	-	-
Sweden	84%	-	-	95%	-	-	84%	-	-	6%	-	-

Source: compiled by the author