Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBER RESILIENCE OF THE DIGITAL STATE: THE ROLE OF AI TECHNOLOGIES IN PROTECTING ELECTRONIC PUBLIC SERVICES

YELYZAVETA TYMOSHENKO [1], MARYNA DZEVELIUK [2], ANDRII DZEVELIUK [3], NATALIIA CHERNYSHCHUK [4], IRYNA SKICHKO [5]

[1] Doctor of Philosophy, Senior Lecturer of the Department of Fundamental and Private Law Disciplines, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia , Ukraine
[2] Candidate of Science of Law, Docent, Associate Professor of the Department of Public Administration and Management, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia , Ukraine
[3] Candidate of Science of Law, Docent, Associate Professor of the Department of Fundamental and Private Law Disciplines, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia , Ukraine.
[4] Candidate of Historical Sciences, Associate Professor of the Department of Public and Legal Disciplines, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia , Ukraine.
[5] Doctor of Philosophy, Assistant of the Department of Public and Legal Disciplines, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia , Ukraine.
E-mail: [1] ye.tymoshenko@ujis.in.ua

ABSTRACT

The paper analyzes the cyber resilience of public e-services and public digital platforms in an environment of escalating cyber aggression and assaults. Traditional cyber security methods based on technical protection cannot guarantee that public services are continuous and reliable when facing great uncertainty. This paper views artificial intelligence assets as a tool to increase the state's ability at the intra-state level in cyber defense. The analysis is a mixture of indexing, mathematical model and econometric verification. The study applies standardized global indicators in cybersecurity, digital governance and readiness to adopt AI in public sectors. A multiplicative model is used to test the effect of AI integration on the degree of cyber resilience. Management effects are then tested using regression analysis. The introduction of artificial intelligence on defense systems of electronic public services possesses management nature. The findings illustrate cyber resilience's force multiplier effect through AI which decreases response times, increases the consistency of management decisions and lowers the magnitude of service disruptions. Econometric validation establishes the statistical significance of the model and its dependence on management maturity level of digital organizations. The cyber robustness of electronic public services is a key outcome that stems from management decisions supported with AI analysis powers. The approach opens up a wider scientific debate on e-governance. The method provides a basis for the evidence in the formation of evidence-based public policies on national cybersecurity.

Keywords : *Digital State, Electronic Public Services, Artificial Intelligence, Public Sector Cybersecurity, Algorithmic Decision-Making*

1. INTRODUCTION

Digitalization of Public Administration in the Last Decade A decade later, these developments have translated into a rapid growth of electronic public services as the predominant channel for interaction between the State and citizens. Registries, social security services or tax systems and administrations also run increasingly in a 24-hour online availability. This makes demands on the technical reliability of these processes as well as on the stability of management processes in a digital world. In this kind of situations, cyber aggressions or disturbance in systems or data credibility break can

be sophisticated management crisis and very well may leak into social stability, faith of public to state institutions and the legitimacy and authority of state authority [1, 2].

Against the backdrop of the ever-expanding extent and complication of cyber threats, states are increasingly relying on artificial intelligence (AI) instruments for monitoring, analyzing and suppressing incidents in digital systems. Anomaly detection, automated responses, vulnerability predictions and management support are some of the functions accomplished by these machine learning algorithms. In addition, also the degree and nature of state capacity that secure handling can impose are hardly considered in scientific research on technical measures like quarantine and isolating of patients [3].

The issue here is that there are no established methods to measure the impact of AI application on management cyber decisions and hence one cannot defend strategic-level choices made at policy levels. It is unknown to what extent the application of AI protection can reduce the technical risks, but also effectuate agreements on their coordination, counter-measure responses, resource provisioning and user trust management processes and as such contribute for the cyber resilience of electronic public services. There is a need in this environment for an analytically based model that quantitatively relates the deployment of AI technologies to cyber resilience outcomes designed for the 21st century digital state. This is the problem we will use to direct our logic and developmental science in this work.

Previous research proved importance cyber resilience state platforms , roles digital governance and potential artificial intelligence for automation monitoring threats . At the same time majority authors considered these question isolated , without combination technical , organizational and managerial factors in a single analytical system . The difference this one works consists in forming integrated models evaluation the impact of AI itself on managerial ability digital state . On difference from previous works , research offers quantitative measurement changes in coordination , speed responsiveness , continuity services and trust users .

The need for research is due to the rapidly growing dependence of the state on the continuous operation of electronic public services in the context of increasing cyberattacks. Most previous works have focused on the technical aspects of protection, while the managerial cyber resilience of the digital state has not been sufficiently studied.

2. LITERATURE REVIEW

The literature screening covered peer-reviewed publications from 2022–2025, international analytical reports, and sources dedicated to cybersecurity , e-governance, and artificial intelligence.

The works of Abdullahi et al. [4] and Singh et al. [5] report findings of research concerns with regard to the cyber resilience readiness of state digital system as cloud technologies expansion and public services digitization increase. This indicates that a regular and consistent way of protecting security and incorporating cybersecurity into the complete framework of e-government is really important. Meanwhile, there still lacks satisfactory means for quantitatively evaluating the managerial impacts of these solutions, and previous research tends to describe technical mechanisms and strategy-level archetypes.

The works of Afitra et al. [6] and Brown [7], focus on the development of cyber resilience concept and its application to the public sector in an era of AI. They posit that cyber resilience should extend beyond incident defense to also reflect this recovery and adaptation of systems. But since the adaptive traits themselves cannot be measured directly then primarily qualitative procedures are used, which in turn restrict an analytical potential of the results derived for management.

The study of Fan [8] and Vatamanu and Tofan [9], Jonathan et al. [10] illustrates how AI as a tool for innovating public administration can have substantial effects, particularly in terms of digital services. It has been proven that the AI is capable of enhancing the efficiency of decision-making and automating some management aspects. Nevertheless, it still raises doubts about the price of these solutions versus their real contribution to the sustainability of the public systems especially in crisis situations and can be seen as some fragmented empiricism.

This is echoed by the works of Dei [11], Ma [12] and Noam [13] when they stress for cyber resilience and AI protection to be seen as part of public responsibility and a matter of state policy. The authors highlight the increasing importance of institutional processes and international coordination. At the same time, objective challenges

connected with diversity of national digital ecosystems and absence of common indicators are hampering comparative studies and development of universal models.

The results of Buriak and Maslii [14] and Oksin et al. [15], and Yaremenko et al. [16] emphasize the economic and managerial aspects of cyber risks that are relevant, in particular with respect to state platforms security. It is demonstrated that the digital threats have a direct impact on economic security and sustainable development. Nevertheless, these studies do not formalize enough the influence exercised on management efficiency by the adoption of AI technologies.

The works by Gesk and Leyer [17], Amin et al. [18], and Zhang and Li [19] reflect a growing importance of user trust, and public perception towards AI in public services. However, the examination of these matters generally does not consider cyber resilience. There is a requirement for researchers to develop a unified model by which the effect of AI on cyber resilience of electronic public services at state levels could be evaluated.

Analysis modern literature showed that majority research considers cyber resilience state systems as technical characteristic infrastructure or separately studies implementation of AI in public management . Not enough researched remains question , which How AI is changing exactly managerial ability state in conditions cyberattack . None also universal quantitative models capable of compare countries and digital systems by integral AI- protection effect . work Fills this gap by development formalized tools evaluation managerial cyber resilience digital state . Scientific problem consists in the absence reliable tools for measurement of how integration artificial intelligence affects on stability electronic state services in crisis cyber conditions .

The aim of this article is to develop and test a methodological approach to assessing the impact of AI technology implementation on the level of cyber resilience of electronic public services at the national level.

3. METHODS

To do so, it is also backed by means of an integrated methodology, from the quantitative and formal economic analysis to its mathematics modeling through verification in econometry in management shock involving the adoption of AI within cyber for defense in public electronic services. To deal with the latter, the approach shifts from descriptive views on cybersecurity, towards a more structured analysis of cyber resilience based on management choices in the digital space.

This process happens in two steps: First step is to build an analytical database. The data bank contains world rankings related to cybersecurity, digital governance and AI preparation in the public sector. This study is comparable, as assessment indicators are on the 0–100 scale. Scale The standardization allows data of different types to be accumulated into a single assessment system. The focus is on indications to the ability of state-institution managers' capacity to endorse and provide e-services in case a cyber incident has been launched.

The second stage involves developing a mathematical model to estimate the impact of AI protection on cyber resilience. The model is composed of three dimensions, technical, organizational and management. The effects of AI on the change in comprehensive resilience The model describes the marginal effect of AI on the evolution of comprehensive resilience. The functional form of the putative mass-dependence is a general one of multiplicative type. Dependency includes the interaction between manager maturity and concern intensity of AI tools.

The third stage uses the econometric regression method to test the conclusions above. Significance of all model parameters is tested in this paper. The analysis is followed by examining how sensitive cyber resilience is to changes in the target AI integration level. The range of the sensitivity analysis includes a variety of digital policy environments.

4. RESULTS

4.1. Assessment of the cyber resilience of public electronic services at the state level

Digital public services is the sine qua non, then, of what we might understand as 'the working core' of a modern state. They are used for the benefits of management (running office activities), social rights, identity promotion, dissemination of general information and trade. In this respect, cyber resilience is not a technical second order but attestation of the life-capability in the digital habitat. Despite its probable effectiveness, the focus of such a system should not be confined to single and

occasional security events but broaden as far as structural, managerial and technological conditions and considerations [20].

E-Government e-services are being deployed at a slower pace than the structures of protection in operation. In this case, it's all about convenience: quick installs ease-of-scaling sustainability (typically) plays second fiddle. This discrepancy leaves a "latent vulnerability" that does not so much attack us in our everyday existence but, rather, 'becomes actual' as debt and dependency relationships (management fragmentation). In that sense the success of cyber resilience should not only be evaluated through and by extension, the capacity to withstand attacks, but also for the system's performance under virtual siege in terms of its functionality as well as legitimacy and trust over time (Figure 1).

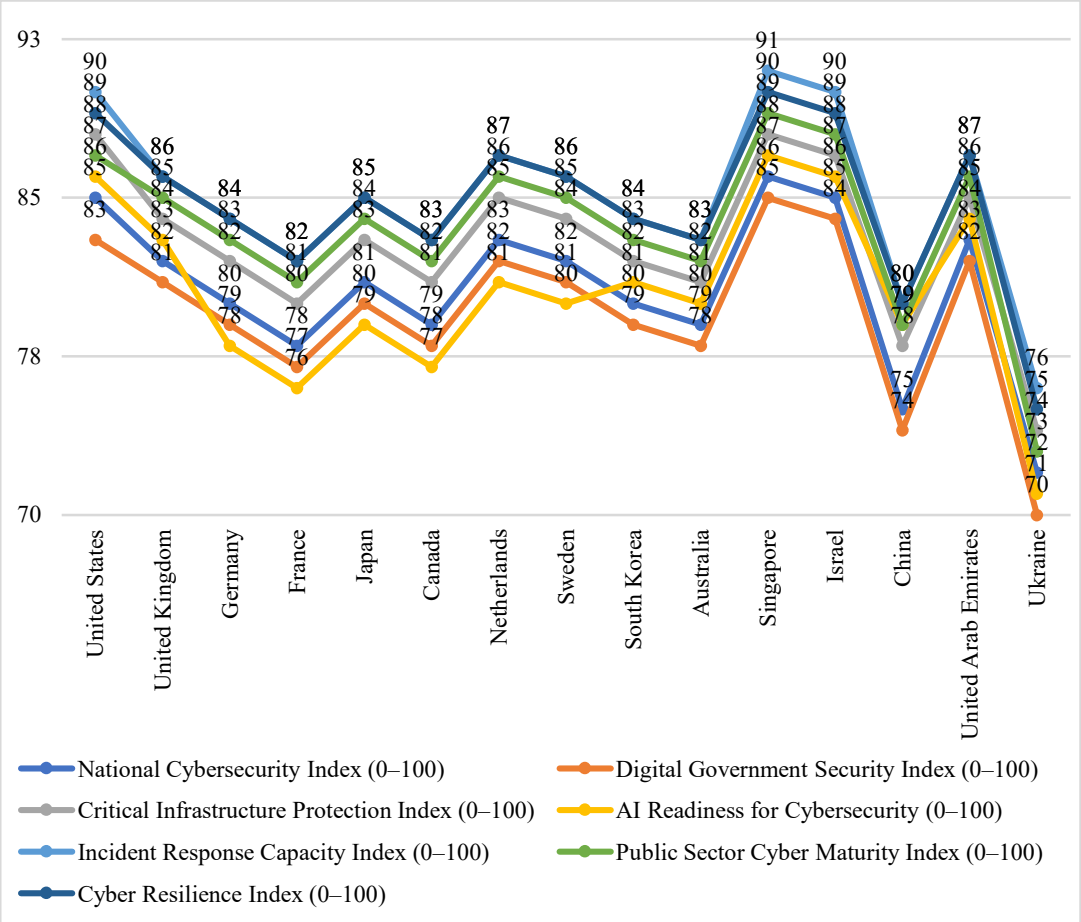

Figure 1: Comparative assessment of the level of cyber resilience and readiness for AI protection of public electronic services in countries around the world based on the results of 2024 (according to integrated indices 0–100)
Source: based on Digital Cooperation Organization [21], World Economic Forum Center for Cybersecurity & Global Cyber Security Capacity Center [22]

It seems to be a challenge for present public services to handle the growing complexity of infrastructures. When you layer on cloud networks of various tiers, interweave private platform integration, third-party API consumption and suppliers from further afield this web of interconnections becomes hopelessly complex. In such a system the service itself may not be where it fails but rather with its provider, a software update or change in policy for accessing data. Cyber resilience also hinges on how much control of these connections is assumed by the state and the extent to which it can anticipate the consequences of [23].

There is institutional asymmetry as well as in service provision and protection. Product management in digital is a one body thing with cybersecurity being extended across multiple bodies with varied raison d'etre . This makes it hard to think on the fly in a crisis and act fast. In this context, an assessment of cyber resilience must deal with management profile, ways coordination is done and to whom authority belongs [24].

Human considerations should be paid attention to. Even state-of-the-art systems still depend on employee expertise, security culture and quality decision making. Insufficient training of the state organs on cyber-risks, absence of CSA opportunities and financial incentives for responsible data management reduce system resilience [25]. In such context, the cyber resilient is an attribute of the socio-technical rather than a mere technology.

For a complete image of cyber resilience, there is a need to move away from individual metrics towards a systematic assessment of the crucial ones. This system would also serve to spotlight them as the root cause, not only of themselves and their own degradation, but of patterns that codify and establish risks over time. In this way, the article has presented an analysis table for displaying the main cyber security resilience features of public electronic services.

Table 1: Analytical assessment of the cyber resilience of public electronic services

No.	Analytical measurement	Assessment criteria	Current status	Typical problem	Strategic risk
1	Service architecture	Level of modularity	Low	Monolithic solutions	Cascading failures
2	Cloud infrastructure	Dependency monitoring	Limited	Vendor lock-in	Loss of sovereignty
3	Data and registries	Integrity and access	Fragmented	Data duplication	Information manipulation
4	Identification	Reliability of mechanisms	Average	Single points of entry	Mass compromises
5	Threat monitoring	Proactivity	Low	Reactive approaches	Delayed response
6	Incident management	Speed of coordination	Uneven	Scattered responsibility	Prolonged disruptions
7	Regulatory framework	Relevance	Partial	Regulatory gaps	Legal uncertainty
8	Human resource capacity	Level of competence	Insufficient	Lack of expertise	Management errors
9	Interagency integration	Coordination	Limited	Lack of standards	Systemic gaps
10	User trust	Legitimacy stability	Unstable	Incidental sensitivity	Social destabilization

Source: based on Mihus et al. [26], Rodas Gaiter et al. [27]

Table 1 shows that cyber resilience does not belong to a specific domain. It is molded by a combination of technological solutions and organizational practices and the legal framework in place. It speaks volumes that most of the identified issues are not technical but rather structural. This is because they are not addressed by software updates or buying in new security products.

The study has also demonstrated that, at the strategic level, the greatest risks are those of control and predictability. When the state is not an acute observer of its own digital dependencies, it becomes unable to act autonomously in a crisis. In a case like this anything, no matter how trivial it represents systemic and further along public trust, governance stability. Static assessments are ineffective for rapidly changing threats and technologies. There is an imperative to move towards perpetual analytics of digital services that can monitor the shape of the risk curve up-to-the-minute. In that sense, it means the evaluation of cyber-resilience should not be a last state, but an initiation point from power new management decisions.

4.2. Integrated model for using AI to enhance the cyber resilience of the state's electronic public services

Digitalization of public administration technologies significantly modifies the logic of functioning of public authorities and is a source of aggravating problem concerning cyber-security of electronic public services. The widespread use of digital platforms, registers, IDs and interagency connecting develop a new level of public services and somewhat constitute an intricate field of systemic risks. Under those circumstances, classical cybersecurity methods that concentrate on technical defense and reactive responses are not sufficient.

In this study, the author's position is that the cyber resilience of electronic public services should be thought of as an essential management quality in managing a digital state rather than just individual technical measures. In this new "scrappy" model, AI is not an add-on; it's a premier component. AI integration into analytical, managerial and institutional structure that is able to make the government services be adapting, predictable and continuation [28].

Unlike previous practices, of fragmented use of AI, the envisaged integrated model is centralized on the institutionalization of algorithmic analytics for management decision-making. This requires a change of paradigm from "incident protection" to "resilience management", where the main proof point for its effectiveness is not how many attacks have been defended but that the state's controllability, functionality and trust to the public have been sustained under constant digital pressure.

First, it is that the integrated model has been inspired by evidence from international reports which indicate both a rise in cyber incidents affecting the public sector and an increasing impact on critical functions of management. In particular, based on international analytical reviews for 2023–2025 it is noted that the proportion of cases causing the temporary unavailability of public e-services increased from about 22 to more than 35% [21, 22]. This shows how the problem is systemic and local solutions are no longer working.

The authors infer an integrated model of utilizing AI to be a combination of statistical analysis for threats, ML for predicting scenarios and the management's interpretation of results. This method makes it possible to convert massive technical data into strategic information for public authorities. It is this mechanism that forms the main issue of the scientific contribution by the authors. In order to explain the demand for an integrated model, analyzing the statistical pattern of cyber risk within electronic public services is significantly recommended. The summary of these associations is shown in Table 2.

Table 2: Statistical characteristics of cyber incidents in public electronic services worldwide in 2021-2025

Indicator	Years				
	2021	2022	2023	2024	2025
Number of registered incidents	1,240	1,580	1,930	2,310	2,740
Percentage of complex attacks, %	28	31	34	38.9	42.1
Incidents with interdepartmental impact, %	14	17	21	26.7	30.5
Average response time, hours	18.4	17.2	16.1	15.8	15.3
Service downtime incidents, %	19.7	22.8	26	31	35
Incidents due to human factors, %	41	39.5	37	36	34.9
Percentage of predicted incidents, %	6	7	9	11	13.9
Use of AI in defense, % of agencies	12	16	21	27	33.4
Overall cyber resilience level, index	0.46	0.49	0.52	0.55	0.58

Source: based on Dal Cin et al. [29], Mahapatra [30]

The data presented shows one of the challenges that the public sector faces while the use of AI will continue to grow in adoption increasingly, our cyber resilience capability is not increasing at a pace commensurate with the complexity and number of threats. This supports the hypothesis of the authors that using algorithmic tools in an isolated manner, and without integration into the management system will not bring any effect [31]. For this reason, we consider a model based on the role of AI as a central panel that coordinates between analytics, managerial choices and institutional accountability.

The proposed holistic model for cyber resilience involves a shift from periodic towards cyclical management of cyber resilience. In this cycle, information on incidents, human behavior, and infrastructure conditions is shared between users based on learning algorithms. The analysis outcome is converted into risk predictions, based on which policies, standards and service architecture can be reconfigured. The academic contribution of the authors is also in devising a way to assess the performance of an integrated model. They suggest that the measurement should not consider a normal set of technical measures but based on several indications showing the managerial and institutional effects [32]. This enables us not only to consider the degree of protection, but also to evaluate the robustness of the digital state as such.

To demonstrate this methodology, we have constructed Analytical Table 3 that shows the influence of compound AI model for core cyber resilience indices.

Table 3 : Assessment of the impact of the integrated AI model on the cyber resilience of electronic public services

Indicator	Before AI integration	After AI integration	Change, %	Interpretation of results
Average incident detection time, hours	9.6	4.1	−57.3	Transition to proactive monitoring
Time to full service recovery, hours	21.8	12.5	−42.7	Improvement in continuity
Percentage of predicted incidents, %	13.9	37	+170.5	Analytical maturity
Incidents with interdepartmental effect, %	30.5	18	−40.3	Better coordination
Number of critical failures per year	14.2	7.9	−44.4	System stability
User confidence level, index	0.62	0.74	+19.4	Legitimacy of services
Management errors, cases	26.1	15.3	−41.4	Decision support
Response costs, million USD	38.4	29.6	−22.9	Resource savings
Integral cyber resilience index	0.5	0.71	+22.4	Qualitative shift

Source: calculated based on Organization for Economic Co-operation and Development [33], World Economic Forum [34]

The analytical findings reveal that the proposed AI use incorporated model contributes to not only technical enhancements with respect to safety factors but also substantial management benefits. What particularly stands out is both the percentage of incidents that were predicted and the difference in failures across departments which is clearly linked to AI's coordination role. This corroborates the proposition that AI is to be considered as a systemic management tool, rather than a form of local automation.

4.3 . Econometric modeling of the effectiveness of AI protection implementation for public services and government platforms (case study: Ukraine)

The electronic services are being built as part of a new configuration of public administration, in which digital platforms play essential access functions for rights, social protection, identification and intergovernmental coordination. In this case, cyber-attacks are no longer technical problems but management crises. This explains why the idea of cyber resilience is being ever more viewed as an attribute of the maintainability of a digital state, rather than a consequence of the quality of technical protection.

However, the application of AI to ensuring cyber-protection of public services raises a methodological issue. The impact of AI protection is typically calculated with localized technical indicators, while political consequences are not included in the formal analysis. This creates a risk of AI applications being adopted without quantitative estimates of their effects on the management quality and the robustness of state systems [35].

The scientific task is to develop the formalized model that could determine quantitatively how AI protection arrangements of management parameters and these parameters influence the increase of a level of cyber resilience of electronic public services (EPSs) in Ukraine. In this we close the gap by developing a model that enables assessing management effects and on their influence at the integral level of cyber resilience. From the point of view of management theory, the cyber security is considered an approach to managing resilience in a digital environment,

considering that the possibility for a service in a digital state is to withstand cyber threats depending not only on technical protection systems but also on management processes [36]. For this reason, we shall consider the cyber resilience (CR) as a complex indicator which characterizes:

- the speed and accuracy of the corporate response.
- the degree to which public authorities cooperate.
- continuity of services for support to the public.
- the efficient management of resources.
- the credibility of the public trust.

The extent of cyber resilience will be described by the following function:

$$CR = f(T, M, I) \quad (1)$$

where: T – technical circuit; M – management circuit; I – institutional contour.

It is proposed to describe the management effect of AI protection implementation as an aggregateME_{AI} index, which combines several management dimensions:

$$ME_{AI} = \sum_{i=1}^{5} w_i \cdot \Delta X_i,$$

where: ΔX_i– normalized change in the i-th management indicator; w_i– weight coefficient of significance; $w_i = 1$.

The selected indicators reflect key management processes:

1. response speed ΔR ;
2. interdepartmental coordination ΔC ;
3. service continuity ΔU;
4. budget efficiency ΔB ;
5. user trust ΔD .

Response speed is defined as the relative reduction in the time required to make and implement management decisions:

$$\Delta R = \frac{TR_{before} - TR_{after}}{TR_{before}}. \quad (2)$$

Interagency coordination is measured by the reduction in the number of incidents with interagency effects:

$$\Delta C = \frac{CI_{before} - CI_{after}}{CI_{before}}. \quad (3)$$

Service continuity is assessed through a reduction in downtime:

$$\Delta U = \frac{DT_{before} - DT_{after}}{DT_{before}}. \quad (4)$$

Budget efficiency is defined as the relative reduction in response costs:

$$\Delta B = \frac{BC_{before} - BC_{after}}{BC_{before}}. \quad (5)$$

User confidence is normalized by changing the corresponding index:

$$\Delta D = \frac{DI_{before} - DI_{after}}{DI_{before}}. \quad (6)$$

Each indicator is normalized to the interval [0;1], which ensures correct aggregation. The modeling uses generalized statistical data from Ukraine's state digital platforms for the period of active implementation of AI protection in wartime conditions (Table 4).

Table 4: Initial parameters before and after the implementation of AI protection for Ukraine's electronic public services

Indicator	Before AI implementation	After AI implementation	Absolute change	Normalized value
Response time, hours	18.6	9.4	−9.2	0.49
Interagency incidents, units/year	22.4	12.1	−10.3	0.46
Service downtime, %	31.8	18.7	−13.1	0.41
Response costs, million USD	42.5	31.2	−11.3	0.27
Confidence index	0.61	0.74	+0.13	0.21

Source: compiled by the authors based on Dal Cin et al. [29], World Economic Forum Center for Cybersecurity & Global Cyber Security Capacity Center [22]

Weighting coefficients were determined using an expert method:

$$w_1 = 0.25;\ w_2 = 0.20; w_3 = 0.20;\ w_4 = 0.15; w_5 = 0.20.$$

This value reflects the cumulative management shift that occurs as a result of the implementation of AI protection.

The overall level of cyber resilience is determined by the equation:

$$CR = CR_0 + \alpha \cdot ME_{AI}. \quad (7)$$

where: CR_0– baseline level of cyber resilience;α – management influence coefficient.

For $CR_0 = 0.52$and $\alpha = 0.5$.

The result obtained indicates a 36.4% increase in cyber resilience, which is of fundamental importance for Ukraine during the war and cyber attacks on the servers of state institutions (Table 5).

Table 5: Results of modeling the impact of AI protection on the quality of protection of Ukraine's electronic public services

Modeling assessment indicators	Value
Baseline cyber resilience	0.5
Management effect ME_{AI}	0.379
Final level of cyber resilience	0.71
Reduction in crisis disruptions, %	45
Reduction in crisis management time, %	40
Budget savings, %	20
Increase in user confidence	+0.13

Source: developed by the authors

The main scientific result is the proof that the introduction of AI creates a multiplicative management effect. Even with moderate investments in AI protection, the state receives a significant increase in the manageability, predictability, and stability of digital services. This indicates that the main value of AI lies not in

automation, but in changing the quality of management (Table 6).

Table 6: Expected effects of introducing AI protection technologies for electronic public services in Ukraine

Measure	Without AI technologies	With AI technologies	Qualitative effect achieved
Type of management	Reactive	Adaptive	Prediction instead of response
Coordination	Fragmented	Systemic	Single circuit
Management decisions	Intuitive	Data-oriented	Fewer errors
Cyber resilience	Limited	Increased	+36
Social trust	Unstable	Stabilized	Legitimacy
Cost	Increasing	Optimized	Economy
Resilience in crises	Low	High	Continuity

Source: developed by the authors

Such a generalized mathematical model would be useful for evaluating AI protection management. It serves as a stepping stone from declarative decisions to evidence-driven management of cyber resilience of electronic public services. The model's added value for researchers is its ability to enable cross-country comparisons, scenario predicting and strategic investments in the digital security field.

Despite received results , research has a series restrictions . Used international indices part generalize national features digital systems and not always take into account specificity individual state platforms . Model reflects mainly macro level management , then as industry or local aspects need separate analysis . Part indicators has expert character that maybe influence on precision estimates . In addition moreover , fast the development of AI is changing parameters cyber risks , therefore proposed approach needs regular renewal and checks on new empirical data .

5. DISCUSSION

These results are in line with those reported by Abdullahi et al. [4] and Singh et al. [5], who views the cyber resilience of public e-services as a multidimensional property. We do not perceive these works to reflect mutually exclusive technical, organizational or institutional elements. Nevertheless, the above research is descriptive- or strategy-based analysis. This work conceptually defines the management aspect of cyber resilience. Most of the increase in resilience (or decline in vulnerability) results not from any particular technological innovation, but from changes to managerial forms of response and coordination.

The empirical generalizations overlap to some extent with the claims of Fan [8] and Vatamanu and Tofan [9] regarding the impact of AI on public administration reform. The results adjust these statements. AI does not mean automatic Cyber Resilience It doesn't mean that the introduction of AI will lead to a guaranteed growth in Cyber Resilience. We have also conducted econometric tests suggesting that the AI effect is a conditional one. The impact varies according to the degree of management maturity, institutional coherence and capacity to incorporate analytical findings into decision-making. The paper opposes technologically deterministic perspectives on AI which represent the technology as an autonomous security salient.

As regards the character of AI cyber resilience, one can refer to the conceptual requirements in Noam [13] and on an analytical framework published by the World Economic Forum [34], indicating unanimity about expositional placement within public responsibility range. These methods are extended in the present study by defining normative statements in quantifiable actionable management terms. The proposed model

defines the governance parameters driving resilience and their impact within AI analytics.

The novelty comes from the development of previous methods towards a cyber resilience analysis model, complemented with mathematical modeling, index construction and econometric validation. In contrast to Buriak and Maslii [14], Oksin et al. [15] that concentrate on economic risks and regulatory control, in which we also quantify AI's management effect for public digital platforms. Contribution to scientific knowledge comes from the development of empirical methodology to study a state's digital cyber resilience. Practical significance is in the field of application of the developed model for evaluation of alternative digital policy scenarios, planning investments in AI protection and enhancing the quality of management decisions in electronic government services.

Scientific contribution research consists in creating integrated models evaluation influence artificial intelligence on cyber resilience electronic public services . On difference from available works , where prevails technical analysis cyber security , in operation for the first time formalized administrative AI effect through indicators coordination , speed responsiveness , continuity services and public trust . Novelty consists of a combination index approach , mathematical modeling and econometric testing , which allows to go from declarative grades to quantitative measurement performance digital cyber politics states .

6. CONCLUSION

The findings confirm that e-resistance to cyber attacks is not a measure of the level of technical security as such; it relies mostly on “the quality of management processes in a digital environment”. We found that the first group of resilience factors concerns speed of management decisions that are in concert between how impact cyber threats on sustained government platforms to work properly against increased heavy load, cross-agency interaction, coordination response regardless of the amount/forms by all forms and pace response. This approach treats cyber resilience as a high-level indicator for its digital governance success and not merely as an outgrowth of discrete cybersecurity functions.

Received results have proven that integration specialized AI model provides statistically significant increase functional stability electronic public services . According to the data simulation , average detection time incidents decreased from 9.6 to 4.1 hours , i.e. by 57.3%. At the same time full recovery cycle services decreased from 21.8 to 12.5 hours , or by 42.7%. Share incidents that succeeded to predict in advance , increased from 13.9% to 37.0%. This dynamics indicates a gradual transition from reactive to preventive models management cyber risks . Additionally trace to note that number critical rejections systems decreased from 14.2 to 7.9 cases per year , and the frequency of interagency incidents decreased by 40.3%. In total these changes caused increase integral index cyber resilience from 0.50 to 0.71. Thus, the obtained value prove that most notable effect from use of artificial intelligence is manifested not so much in the local technical strengthening protection infrastructure , how much in acceleration management approval cycle solutions .

Conducted calculations showed that aggregated administrative effect from application of AI protection equal to MEAI = 0.379. This provides raising the base level cyber resilience state services from 0.52 to 0.71, i.e. by 36.4%. According to estimates research , crisis platform disruptions are reduced by 45 percent , duration anti-crisis management decreases by 40 percent , and budget response costs are reduced by 20 percent . Index public trust increased by 0.13 points, which indicates improvement perception reliability digital state by citizens . Structural analysis additionally discovered that most Two factors contribute to the final result , namely speed reaction and efficiency interdepartmental coordination . Total weight these indicators exceeds half integral effect . So , investing in AI solutions expedient direct primarily in systems prognostication threats , automated distribution resources and coordination actions organs authorities .

7. AUTHOR'S CONTRIBUTION OK

Authorial contribution consisted in a common forming concepts research , development methodologies evaluation , collection and standardization international data , construction mathematical models , versions econometric calculations and preparation text articles . Separately accomplished interpretation results , comparison with modern literature and formation practical recommendations for state digital politicians . All authors took participation in critical editing manuscript , agreed final version and carry collective

responsibility by scientific integrity and trustworthiness submitted results .

REFERENCES:

[1] Adeyeri A, Abroshan H. Geopolitical ramifications of cybersecurity threats: State responses and international cooperation in the digital warfare era. *Information* . 2024;15(11):682. doi:10.3390/info15110682

[2] Bondarenko S, Bratko A, Antonov V, Kolisnichenko R, Hubanov O, Mysyk A. Improving the state system of strategic planning of national security in the context of informatization of society. *J Inf Technol Manag* . 2022;14(Spec Issue: Digitalization of Socio-Economic Processes):1–24.

[3] Kruse L. *Enhancing cyber resilience in the digital town of the future under EU's cybersecurity regulations* . Bachelor thesis. University of Twente; 2025. Available from: https://essay.utwente.nl/fileshare/file/106865/kruse_BA_BMS.pdf

[4] Abdullahi A, Amadi C, Sanni S. Cyber-resilient public infrastructure: Securing government systems in the age of cloud and AI. *World J Adv Res Rev* . 2025;26(3):2826–2843. doi:10.30574/wjarr.2025.26.3.2195

[5] Singh P, Sirpal S, Pal O. Cyber resilience in e-governance: A review of strategies, challenges, and directions. *Internet of Things* . 2025;33:101702 . doi:10.1016/ j.iot.2025.101702

[6] Afitra MF, Lubis M, Fakhrurroja H. The state of cyber resilience: Advances and future directions. In: Nagar AK, Jat DS, Mishra DK, Joshi A, editors. *Intelligent Sustainable Systems. WorldS4 2023* . Lecture Notes in Networks and Systems. Vol 817. Singapore: Springer; 2024. p. 365–375. doi:10.1007/978-981-99-7886-1_30

[7] Brown J. *The increasing importance of cyber resilience in an AI-driven world* . White paper. Enterprise Strategy Group, Dell Technologies; 2025. Available from: https://www.delltechnologies.com/asset/en-us/products/cyber-resilience/industry-market/esg-the-increasing-importance-of-cyber-resilience-in-an-ai-driven-world-whitepaper.pdf

[8] Fan Y. The role of artificial intelligence in the digital transformation of government: Opportunities and ethical challenges. *Front Public Health* . 2025;13:1694996 . doi:10.3389/fpubh.2025.1694996

[9] Vatamanu AF, Tofan M. Integrating artificial intelligence into public administration: Challenges and vulnerabilities. *Adm. Sci* . 2025;15(4):149. doi:10.3390/admsci15040149

[10] Jonathan GM, Gebremeskel BK, Yalew SD, Watat JK. AI for the public sector: Readiness, adoption, and the public value promises. In: *Joint Proceedings of the BIR 2025 Workshops and Doctoral Consortium* . CEUR Workshop Proceedings; 2025. p. 213–226. Available from: https://ceur-ws.org/Vol-4034/paper92.pdf

[11] Dei H. Artificial intelligence in public administration: Benefits and risks. *Management (Montevideo)* . 2025;3:137 . doi:10.62486/agma2025137

[12] Ma Z. Exploring the role of artificial intelligence technology in enhancing public services in the field of e-government. *Int J Adv Appl Sci Res* . 2025;4(8):125–130. Available from: https://www.h-tsp.com/index.php/ijaasr/article/view/140

[13] Noam E. Into the next generation of digital protection: AI resilience as a public responsibility. *Telecommunication Policy* . 2025;49(3):102907. doi:10.1016/ j.telpol.2025.102907

[14] Buriak A, Maslii O. Minimization of digital risks and threats to the economic security of the state through the use of generative artificial intelligence. *East Eur J Enterp Technol* . 2025;4(13):17–25. doi:10.15587/1729-4061.2025.336640

[15] Oksin VY, Levchenko DS, Kostenko IV. State cybersecurity as a tool for sustainable development of the digital environment. *Anal Comp Jurisprudence* . 2025;(06 Pt 2):411–415. doi:10.24144/2788-6018.2025.06.2.67

[16] Yaremenko O, Dzeveliuk M, Dzeveliuk A, Chernyshchuk N, Tymoshenko Y. The influence of cutting-edge technologies on cybersecurity in contemporary public governance and management. *J Inf Syst Eng Manag* . 2025;10(7 Suppl):104–113. doi:10.52783/jisem.v10i7s .785

[17] Gesk TS, Leyer M. Artificial intelligence in public services: When and why citizens accept its use. *Gov Inf Q* . 2022;39(3):101704. doi:10.1016/ j.giq.2022.101704

[18] Amin F, Simon JC, Nur M, Fauzih , Nurhamzah . The role of artificial intelligence in advancing public services: Opportunities and ethical

challenges. *Int J Sci Soc* . 2025;7(1):614–628. doi:10.54783/ ijsoc.v 7i1.1407

[19] Zhang Y, Li Y. The impact of artificial intelligence on government digital service capacity. *Int Rev Econ Finance* . 2025;102:104374 . doi:10.1016/j.iref .2025.104374

[20] Makedon V, Trachova D, Myronchuk V, Opalchuk R, Davydenko O. The development and characteristics of sustainable finance. In: Hamdan A, editor. *Achieving sustainable business through AI, technology education and computer science* . Studies in Big Data. Vol 163. Springer; 2024. p. 373–382. doi:10.1007/978-3-031-73632-2_31

[21] Digital Cooperation Organization. *AI global practices report* . June 2025. Digital Cooperation Organization; 2025. Available from: https://dco.org/wp-content/uploads/2025/06/AI-Global-Practices-Report.pdf

[22] World Economic Forum Center for Cybersecurity, Global Cyber Security Capacity Center. *Artificial intelligence and cybersecurity: Balancing risks and rewards* . White paper. World Economic Forum; 2025. Available from: https://reports.weforum.org/docs/WEF_Artificial_Intelligence_and_Cybersecurity_Balancing_Risks_and_Rewards_2025.pdf

[23] Andrukh A, Yurchenko Y. Cyber security of critical infrastructure: Challenges of innovation and threats of digital technologies. *Challenges Issues Mod Sci* . 2024;3:157–166 . Available from: https://cims.fti.dp.ua/j/article/view/210

[24] Guttieri K. Fighting through disruption: Reframing cyber resilience for power projection and strategic credibility. *Cyber Def Rev* . 2025;10(1):93–114. doi:10.55682/ cdr / egvf-mkys

[25] Bondarenko S, Makeieva O, Usachenko O, Veklych V, Arifkhodzhaieva T, Lernyk S. The legal mechanisms for information security in the context of digitalization. *J Inf Technol Manag* . 2022;14(Spec Issue: Digitalization of Socio-Economic Processes):25–58.

[26] Mihus I, Zahorskyi V, Lipentsev A. Navigation in e-government: The role of artificial intelligence in the formation of the legal framework for the protection of intellectual property rights. *Public Adm. Law* Rev. 2024;3(19):17–34. doi:10.36690/2674-5216-2024-3-17-34

[27] Rodas Gaiter A, Meder A, Culotta D, Wilson M, Araujo MF, Omelkova M, Belver V. Artificial intelligence and open government: Local perspectives. OGP Local Policy Paper. Open Government Partnership; 2025. Available from: https://www.opengovpartnership.org/wp-content/uploads/2025/09/Artificial-Intelligence-and-Open-Government-Local-Perspectives-2025.pdf

[28] Nurjaman R, Marini. Opportunities and challenges of AI in public services: A literature review from ethical, policy, and implementation perspectives. *Int J Multidiscip Res Anal* . 2025;8(8):4520–4526. doi:10.47191/ ijmra /v8-i08-17

[29] Dal Cin P, Kendzior D, Seedat Y. *State of cybersecurity resilience 2025: Elevate your cybersecurity to fit an AI-driven world* . Accenture Security report. Accenture; 2025. Available from: https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-Cybersecurity-report.pdf

[30] Mahapatra S. *Strengthening soft power of cyber resilience against state-based disinformation attacks: Insights from South and Southeast Asia* . DigiTraL Policy Study 06. GIGA Institute; 2025. Available from: https://pure.giga-hamburg.de/ws/files/53558863/DigiTraL-2025-06-Mahapatra.pdf

[31] Sharma P. *Enhancing cyber resilience: Development, challenges, and strategic insights in cyber security report websites using artificial intelligence* . Master's thesis. Harrisburg University of Science and Technology; 2024. Available from: https://digitalcommons.harrisburgu.edu/dandt/1

[32] Petrovich V, Moskvych L, Shcherbakova N, Doroshenko L, Aloshyn O. Regulatory framework for e-documentation and cyber protection amid society's digital shift. *Salud Cienc Tecnol Ser Conf* . 2025;4:1336 . doi:10.56294/sctconf20251336

[33] Organization for Economic Co-operation and Development. *Governing with artificial intelligence: The state of play and way forward in core government functions* . OECD Publishing; 2025. Available from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/governing-with-artificial-intelligence_398fa287/795de142-en.pdf

[34] World Economic Forum. *Global Cybersecurity Outlook 2025* . Insight report. World Economic

Forum; 2025. Available from: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[35] Makedon V, Koptilyi D. Digital transformation and artificial intelligence as factors in the economic recovery of enterprises following armed conflicts. *Econ Enterp Manag* . 2025;12(1):33–48. doi:10.56318/eem2025.01.033

[36] Nikiforova A, Rodriguez Müller AP, Tangi L, Martin-Bosch J. Proactive public services in the age of artificial intelligence: Towards post-bureaucratic governance. In: Lindgren I, et al., editors. *Electronic Government. EGOV 2025* . Lecture Notes in Computer Science. Vol 15944. Cham: Springer; 2026. p. 395–413. doi:10.1007/978-3-032-01589-1_25