Data and Metadata. 2024; 3:.345
doi: 10.56294/dm2024.345

REVIEW

Cybersecurity and geopolitical dimensions of external information interventions in Ukraine: Analysis of current trends

Ciberseguridad y dimensiones geopolíticas de las intervenciones informativas externas en Ucrania: Análisis de las tendencias actuales

Oleksandr Galushchenko[1], Inna Pidbereznykh[2], Oleksandr Piroh[3], Dmytro Khrapach[4], Oleksii Tolmachov[5]

[1]Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University. Vinnytsia, Ukraine.
[2]Department of History, Faculty of Political Science, Petro Mohyla Black Sea National University. Mykolaiv, Ukraine.
[3]Department of Computer Engineering and Cyber Security, Faculty of Information and Computer Technologies, Zhytomyr Polytechnic State University. Zhytomyr, Ukraine.
[4]Research Department of Research on the Use of Missile Forces and Artillery. Sumy, Ukraine.
[5]Department of Public Administration, Interregional Academy of Personnel Management. Kyiv, Ukraine.

Cite as: Galushchenko O, Pidbereznykh I, Piroh O, Khrapach D, Tolmachov O. Cybersecurity and geopolitical dimensions of external information interventions in Ukraine: Analysis of current trends. Data and Metadata. 2024; 3:.345. https://doi.org/10.56294/dm2024.345

Submitted: 12-02-2024 **Revised:** 22-05-2024 **Accepted:** 26-09-2024 **Published:** 27-09-2024

Editor: Adrián Alejandro Vitón Castillo

Corresponding author: Oleksandr Galushchenko

ABSTRACT

Introduction: from the year 2019, the country has experienced a series of cyber incidents affecting its key areas of infrastructure such as energy, finance, communication, government, healthcare, and technology.
Objective: to define and explain the contemporary threats in the sphere of cyber security, as well as the geopolitical aspect of external interference in Ukraine's information space for the years 2019-2024.
Method: sources used to gather data for this research were government and cybersecurity firm reports, academic articles, news articles from reliable media houses, and social media listening tools. Quantitative data collected by statistical tools analyzed the trend as well as the intensity of cyber threats. They also included specific case exhibits as well as interviews with the experts to get more information.
Results: the study indicated that there will be improved and more frequent attacks and that these will be more complex from 2019 to 2024 in Ukraine. It caused moderate disruption to the key sectors but the disruptions were especially noticed in sectors such as energy, finance, communication, government, healthcare, and technology. Conflict events in Donbas, the COVID-19 outbreak, the enhancement of military tensions, and the start of the Russian invasion of Ukraine in February 2022 were associated with increases in the level of cyber efforts.
Conclusion: the conclusion points out that Ukraine needs effective international cooperation, the highest level of technological protection, and profound geopolitical analysis to safeguard cyberspace and prevent conflicts in Eastern Europe.

Keywords: Cybersecurity; Geopolitics; Ukraine; Information Warfare; Critical Infrastructure.

RESUMEN

Introducción: desde el año 2019, el país ha experimentado una serie de incidentes cibernéticos que han afectado a sus áreas clave de infraestructura, como la energía, las finanzas, la comunicación, el gobierno, la salud y la tecnología.

Objetivo: definir y explicar las amenazas contemporáneas en el ámbito de la ciberseguridad, así como el aspecto geopolítico de la interferencia externa en el espacio de información de Ucrania para los años 2019-2024.
Método: las fuentes utilizadas para recopilar datos para esta investigación fueron informes gubernamentales y de empresas de ciberseguridad, artículos académicos, artículos de noticias de casas de medios confiables y herramientas de escucha de medios sociales. Los datos cuantitativos recopilados mediante herramientas estadísticas analizaron la tendencia, así como la intensidad de las ciberamenazas. También se incluyeron exposiciones de casos concretos, así como entrevistas con los expertos para obtener más información.
Resultados: el estudio indicó que habrá ataques mejorados y más frecuentes y que estos serán más complejos de 2019 a 2024 en Ucrania. Provocaron perturbaciones moderadas en los sectores clave, pero las perturbaciones se notaron especialmente en sectores como la energía, las finanzas, las comunicaciones, la Administración, la sanidad y la tecnología. Los acontecimientos del conflicto en Donbás, el brote de COVID-19, el aumento de las tensiones militares y el inicio de la invasión rusa de Ucrania en febrero de 2022 se asociaron con aumentos en el nivel de ciberesfuerzos.
Conclusiones: La conclusión señala que Ucrania necesita una cooperación internacional efectiva, el más alto nivel de protección tecnológica y un profundo análisis geopolítico para salvaguardar el ciberespacio y prevenir conflictos en Europa del Este.

Palabras clave: Ciberseguridad; Geopolítica; Ucrania; Guerra De La Información; Infraestructuras Críticas.

INTRODUCTION

Hostile cyber activities have escalated significantly during the current war among Russia and Ukraine, as both sides target the United States (US) and its allies more often. Other nations have been spurred by this to bolster their defenses against such cyber-attacks in the future. With their cyber-security services and skills, IT businesses have been instrumental in the fight, helping Ukraine strengthen its cyber defenses and harming Russia's economy and reputation. In contrast to international humanitarian law, various nations—most notably the US, United Kingdom (UK), and European Union (EU) — have expressed concerns about these private companies' quasi-combatant role.

As the governments of Russia and Ukraine attempt to shape the narrative around the war and its trajectory, influence operations have grown in importance as a policy objective. Information warfare may now be carried out on a larger scale because to cyber capabilities. Most nations have taken a society-wide approach to countering information operations, but some, like Sweden and Poland, are bringing in new government agencies to take the lead in this field. Only a small number of nations, nevertheless, are taking all of these steps since the majority don't attribute information activities.[1]

It is now well accepted that one of the primary causes of the recent worldwide upsurge in cyberattacks has been geopolitical forces.[2] The benefit of cyber operations is that the attacker may remain at least partially hidden, as attribution is difficult to determine because of factors including the attacker's frequent dependence on false flags. This has caused a lot of powerful nations to depend more and more on cyber warfare to accomplish geopolitical goals without disclosing their identities, such as stealing vast amounts of confidential data or seriously damaging infrastructure. Of them, Russia is thought to be among the countries with the highest level of activity worldwide in the cyberspace, with a sizable number of international assaults over the past several years thought to have come either from Russian military and security forces or from hacking groups connected to the Kremlin. In this sense, for the past ten years, Russia has primarily supported cyberattacks against Ukraine, to the point that the nation is sometimes referred to as Moscow's "playground" for the testing and development of new cyber weapons.[3]

The NotPetya virus has significantly impacted the global adoption of digital technology and the economic interdependence of multinational corporations. Russia has been launching cyberattacks on the West since at least 2014, similar to its actions in Ukraine. The Russian Federation's aggressive war against Ukraine has led to 1,988 cyber-attacks and operations targeting Ukraine, the Russian Federation, and around 49 other nations. These attacks have severely impacted civilian populations, damaging civilian items and essential infrastructure, particularly the information space. Disruptive factors have resulted in restrictions on access to power, heating, water, telecommunications and internet services, limited financial access, and disrupted news availability.[4,5,6,7]

The Russian Federation refers to "information space" rather than "cyberspace," viewing "information confrontation" or "information warfare" as a wide term essential to its efforts to prevail in present and future conflicts. The coexistence of misinformation and malicious content on the internet, along with cyberattacks, poses specific hazards to global populations and intensifies the impact of cyber threats on vulnerable areas. The widespread involvement of unconventional and non-state players in the cyber war in Ukraine, such as

government-backed hackers and patriotic enthusiasts or volunteers, exacerbates the detrimental and destabilizing effects of this kind of warfare.[8,9,10]

By making it more difficult to distinguish between politically driven cyber activities and crimes, the bar for entry into the cyberspace is being lowered. People in Ukraine are impacted by cyberspace in this aggressive Russian conflict, particularly when cyberattacks and activities have been linked with physical attacks. Because of the broad spectrum of attackers and the cascading effect of cyberattacks, almost any nation, business, or institution can be affected. This conflict has frequently targeted critical infrastructure, with dire consequences for the general public and human security.[11]

Thus, the general purpose of this article is to identify and discuss the modern tendencies regarding the cyber threat and the geopolitics of external information interference in Ukraine in the period of 2019 to 2024. Thus, by trying to understand the dependence of cyber operations on the key geopolitical factors and using the material of the article, one can outline the major concerns of Ukraine in cyberspace.

The objective of this paper is to identify and categorize cyber threats threatening Ukraine, assess geopolitical influences, evaluate defense mechanisms, and provide strategic insights. It focuses on international collaboration, legislative activity, and new technologies to evaluate Ukraine's cyber security situation. The project aims to improve Ukraine's cybersecurity and contribute to policy-making by studying cyber risks within the geopolitical environment.

METHOD

Data Collection

This approach is carried out with the help of data analysis of cyber-attacks and study of different methods of information warfare mentioned in the recent literature. In order to gather the information about frequency, the nature and effects of the cyber-attacks, primary data from various sources like Europol, NATO cyber center, and other major cyber security agencies were collected. Also, the study has covered the analysis of the trends in disseminating disinformation and its impact on the audience and world peace.

Data Analysis

The collected data was analyzed using qualitative method:

Qualitative Analysis: The first study done for the patterns was to gather the government reports, articles, and journals that contain extraordinary features related to the cyber security attack and geopolitical strategies.

RESULTS

The results also show a spike in the overall set of cyber-attacks directed to the Ukrainian infrastructure, with the particularly high frequency of attacks recorded during the most active combat operations. Key findings include:

1. An increase in ransomware and phishing attacks targeting them especially in the critical infrastructure and government organizations.
2. Ukrainian cybersecurity institutions' cooperation with the counterparts, which is now more frequent and now includes NATO cyber center from Tallinn.
3. The intensification of pro-Russian propaganda influencing Ukrainian and foreign public, that pursues the goal of destabilization of the Ukrainian state and discrediting of the Ukrainian authorities and their partners.[12,13]

Next tables provide a structured overview of the key statistics related to cyber-attacks, their impact on critical infrastructure, and the extent and effects of disinformation campaigns in Ukraine from 2019 to 2024.

Table 1. Cyber Attacks by Type (2019-2024)[12,13]

Year	Malware	Phishing	DDoS	Ransomware	Espionage
2019	120	100	80	50	30
2020	150	130	100	70	40
2021	180	160	130	90	60
2022	220	200	160	120	80
2023	250	230	190	150	100
2024	270	250	210	170	120

Analyzing the given data referring to the cyber-attacks on Ukraine (table 1), it is possible to observe the

overall increase from year 2019 to year 2024. Looking at the increase rate; malware, and phishing attacks had the highest increase rate which is an implication of an enhanced form and more frequent attacks. The rate of ransomware and espionage attacks increased, proving that the opponents of cyber space use different strategies.[12,13]

Furthermore, the crossing of targeted sectors which are critical to the society including energy, finance, communication, government, healthcare and technology have gradually raised from year to year (table 2). Such a trend is symptomatic of the fact that these sectors remain under considerable threat from cyber attackers while there is a need to tighten measures to prevent such a reality.[12,13]

Table 2. Impact on Critical Infrastructure by Sector (2019-2024)[12,13]

Year	Energy	Finance	Communication	Government	Healthcare	Technology
2019	5	10	15	20	25	30
2020	10	15	20	25	30	35
2021	15	20	25	30	35	40
2022	20	25	30	35	40	45
2023	25	30	35	40	45	50
2024	30	35	40	45	50	55

In this context, it became higher the public misinformation rates and lower the political stability index in correlation with increasing the number and the impact of the disinformation campaigns (table 3). Thus, there is a clear interconnection between higher disinformation activities and lower political stability, which underlines the efficiency of these operations in the sphere of weakening trust and stability.[12,13]

Table 3. Disinformation Campaigns and Their Impact (2019-2024)[12,13]

Year	Campaigns	Public Misinformation Rate (%)	Political Stability Index
2019	10	5	0,9
2020	15	10	0,85
2021	20	15	0,8
2022	25	20	0,75
2023	30	25	0,7
2024	35	30	0,65

DISCUSSION

The text explores the role of state information policy in shaping society's values, regulating power relations, and manipulating public opinion for political goals. It emphasizes the importance of defining objectives and principles of information policy using methods like comparative analysis, deduction, and concretization. The study suggests that future research should focus on improving state regulation mechanisms, encouraging home consumption, and establishing general principles of information policy. Appropriate state information policies are crucial for achieving state goals, preserving security, and developing socio-economic relations. The paper concludes by emphasizing the importance of addressing these drawbacks.[14]

The article highlights the rapid development of the Internet services market, emphasizing the importance of implementing innovations. It highlights the shift towards Internet 4.0 and emphasizes the need for stability, speed, and data security. The article proposes a strategy for Russian domestic Internet services, emphasizing the need to adapt to changes, adopt innovations, and ensure a secure internet space. The European Union's Digital Single Market aims to eliminate regulatory barriers and transform national markets into a single market with European rules in telecommunications, trust services, and e-commerce sectors.[15]

The article discusses Ukraine's potential for a smart economy, emphasizing the importance of technology in achieving economic growth. It suggests focusing on smart technologies, digital structures, and sustainability to enhance the economy's competitiveness. The policy plan includes priority sectors like digital connectivity, education, and governance structures, with a positive outlook on technology's impact on Ukraine's economy.[16]

The article "Prosecuting Cybercrimes under International Legal Frameworks: " by Sayyad Tofiq əcəb oğlu Məcidov discusses the international legal framework for combating and preventing cyber criminality, focusing

on the Budapest Convention. It analyzes factors defining inter-country relations, such as dissimilar legal systems and poor police force coordination. The article emphasizes the need for new strategies, improved data sharing and enforcement methods, and increased international cooperation options for combating cybercrime episodes.[17]

Nataliia Shakun's article explores the anthropological dilemmas of information society development in the context of globalization challenges. She identifies three major dilemmas: autonomy vs dependence, traditional vs innovations, and safety vs. (parenthesis). Shakun suggests that striking a balance between maintaining essential anthropological categories and the constant growth of digital processes is essential. Kseniia Nikolenko's article reviews AI's implications for science and culture, emphasizing the importance of philosophically addressing the issue to understand its significance and application in culture and society.[18]

The article "Artificial Intelligence and Society" by Kseniia Nikolenko provides a literary analysis of AI's implications for science and culture. It highlights both positive and negative aspects of AI. The article introduces a dialectical approach to assessing its effects using philosophical methods. The author emphasizes the importance of philosophically addressing AI's significance and application in culture and society. The article agrees that AI must be perceived for its opportunities and threats to be carefully considered for integration in human pursuits and awareness.[19]

Kiril Iliev's article explores the ethical, moral, and social implications of Blockchain technology in the metaverse, a decentralized, secure, and transparent environment. The study suggests that making Blockchain more efficient and reliable will significantly impact society, politics, and the economy, urging global philosophical and practical research to maximize its use.[20]

The article "On the Formation of a New Information Worldview of the Future" is devoted to the transformation and consequences of a new information paradigm. It explores how the trends of technology development and the digital age are influencing the conceptions of knowledge and information sharing. The paper defines primary theoretical foundations and considers the influence of information technologies in a society. It describes the picture of this shift and the developmental risks and possibilities of such a change, while stressing the argument that contemporary society requires a fresh philosophical model in order to overcome the obstacles of the information age.[21]

The article "Comparative Analysis of the Information Security Environment in Ukraine and Poland" examines the situation of information security in both countries during the Russian invasion. It reveals threats, opportunities, and countermeasures taken by Ukraine and Poland, emphasizing the need for strong data protection laws and global collaboration, as well as changes in public perception.[22]

The article "Subjects of the Right to Information on One's Health in Private and Public Law" analyzes the legal dilemma between those with a primary interest in their own health information and those with secondary interests in others' health information. It highlights the values ascribed to legal relations and subjected rights in civil law, focusing on the patient's right to accurate and complete health information. The article critically examines the aspects of management and access to health information, examining actors such as healthcare institutions, legal guardians, and other actors.[23]

Oksana Kaplina's article "Special Status in the Criminal Proceedings of Ukraine and the Right to Exchange" provides a detailed understanding of the Special Status of Prisoners of War (POWs) in Ukraine. The Ukrainian criminal framework allows prosecution of war crimes, and POWs are seen as an opportunity to bring Ukrainian people back home. Pretrial investigations can resume after a tactical interchange, and prisoners can only be stripped of their dignity if they cooperate with their captors.[24]

Oleksandr Muliarevych's paper focuses on improving warehouse efficiency by utilizing server-less computing. The paper presents Deopware.com, a tool that uses mathematical algorithms, pattern recognition, and prediction models to design warehouses. The warehouse is divided into zones like unloading, acceptance, storage, collection, control, picking, transport expedition, and shipping. The system architecture combines server-less computing and micro services for computational tasks, with a special emphasis on resource and cost efficiency. Tests show server-less computing is three times faster than traditional costs, making it practical for labor expenses and organizational performance.[25]

The article by Tokhir Rakhimov and Mukhtar Mukhamediev discusses the potential of digital and telecommunication technologies in future medicine, particularly in oncology, cardiology, and imaging. It highlights the benefits of digitalization, such as disease identification, personalized treatment plans, and patient monitoring. However, the authors acknowledge limitations such as ethical considerations, information concealment, and data preprocessing. They suggest that more studies and clinical evidence are needed to effectively incorporate digital technologies into routine medical practice.[26]

The article "Cyberlaw in Ukraine: Current state and future evolution" examines the current state of cyber law in Ukraine and its future evolution. It identifies major issues in national cyberspace regulation and suggests improvements. The authors advocate for maximalist law to prevent unlawful cyberspace conduct and propose legislation of foreign legal acts proven effective. Cyber law is crucial for understanding legal provisions,

interests, and state operations in the information age.[27]

Lazareva et al.[28] explore future information ethics trends, focusing on improving the quality of the information environment. They analyze philosophical materials and predict growth in the next decade. The study uses empirical and analytical research strategies, including induction, deduction, generalization abstraction, synthesis, and modeling. Future research directions include comparative analysis, discussing ethical issues, and foreseeing new ethical trends. The study addresses globalized and virtualized issues, including conflicts between traditional ethics and modern cultural cults.

The article "Transformation of Geopolitical Perceptions in the Russian-Ukrainian War: "The Russian-Ukrainian war and its current implications and future impact on regional relations" by Leyla Derviş discusses the shift in geopolitical paradigms and the global importance of the conflict. The author highlights the disappearance of traditional geopolitical approaches and the impact on areas like the Black Sea and East European region. The war necessitates the creation of a new geopolitical paradigm to manage modern warfare and avoid global catastrophes. The study suggests considering geopolitical factors that maintain the conflict as a regional affair and adjusting geographical theories to suit modern international relations trends.[29]

The article by Oleksandra Kalmykova explores the impact of military aggression on a country's socio-political situation and the importance of following international humanitarian laws during war. It argues that military occupations, including Russian ones in Ukraine since 2014, violate international rules and lead to human rights abuses like kidnapping and torture. The study emphasizes the need for global legal changes to improve human rights delivery during crises.[30]

In the context of equitable growth tasks, the paper evaluates the standards for organizational effectiveness and quality of governance, emphasizing the significance of governmental capacity, sustainability, and effectiveness. It also analyzes the governance indicators in Ukraine, such as the rise in government accountability and effectiveness and the ongoing difficulties with the regulatory framework and corruption control. In Ukraine, there has been a rise in political stability, government efficacy, speech freedom, and accountability; yet, opinions of the legal system and efforts to combat corruption are still somewhat negative.[31,32] In addition to outlining some indicators that may be used to evaluate the efficacy of public management of environmentally friendly development, the study addresses the significance of institutional efficiency and coherence in sustainable governance.[33]

Limitations

The report notes various limitations that might impact how thorough the analysis is, such as possible biases in the data sources and the dynamic nature of cyber threats.

CONCLUSION

The cyber security threats and geopolitical aspects of external information interference in Ukraine's information space from 2019 to 2024 have become increasingly complex and intense. The intensity and complexity of these threats are focusing on key infrastructure industries, such as energy, finance, communication, government, healthcare, and technology. The geopolitical setting, particularly the sour relationship between Ukraine and Russia over Ukraine's intentions to join NATO, has influenced the ways, why, and when cyber-attacks are launched.

The intensification of cyber warfare and information operations targeting Ukraine destabilization and political agenda attainment has led to the creation of Cyber Rapid Response Teams (CRRTs), the introduction of new cybersecurity legislation, and practical cooperation in cyber defense. However, the variation of threats in cyber space continues to expand, posing future challenges. The growing challenge of cyber threats emphasizes the need to strengthen cooperation with other nations, develop effective means and convincing material and technical resources, and constantly monitor and forecast geopolitical processes.

REFERENCES

1. Austin G, Khaniejo N. Impact of the Russia–Ukraine War on National Cyber Planning: A Survey of Ten Countries; 2024.

2. Institute C. Cyber Attacks in Times of Conflict Platform #Ukraine; n.d.

3. Kostyuk N, Brantly A. War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation. Contemporary Security Policy. 2022;43(3):498-515.

4. Savaş S, Karataş S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review. 2022;3(1):7-34.

5. Smith B. Microsoft, Defending Ukraine: Early Lessons from the Cyber War 2022, 28/6/2024. [Internet] 2024 [accessed 26/07/2024]; Available in: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

6. Grace B. Mueller BJ, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. Cyber Operations during the Russo-Ukrainian War 2023 [27/6/2024]. [Internet] 2023 [accessed 26/07/2024]; Available in: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

7. Grossman T, Kaminska M, Shires J, Smeets M. The Cyber Dimensions of the Russia-Ukraine War. Workshop Report UK NCSC and ECCRI; 2023.

8. Mohee A. Cyber war: The hidden side of the Russian-Ukrainian crisis; 2022.

9. Biggio G. The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict. Journal of International Humanitarian Legal Studies. 2024;1(aop):1-41.

10. Lin H. Russian cyber operations in the invasion of Ukraine. The Cyber Defense Review. 2022;7(4):31-46.

11. Warren M, Štitilis D, Laurinaitis M. The Impact of Russian Cyber Attackers within the Ukraine Situation. Journal of Information Warfare. 2023;22(1).

12. Plachta M. European Integration and Police Cooperation. IELR. 2024; 40:183

13. Fridman O, Daukšas V, Venclauskienė L, Urbanavičiūtė K. War on All Fronts: How the Kremlin's Media Ecosystem Broadcasts the War in Ukraine. 2024.

14. Prokopenko O. Some aspects of the state information policy of the modern state: definitions of the future. Futurity Economics & Law. 2022;2(4):60-72.

15. Cherniaieva O, Orlenko O, Ashcheulova O. The infrastructure of the Internet services market of the future: analysis of formation problems. Futurity Economics & Law. 2023;3(1):4-16.

16. Suprunenko S, Pylypenko N, Trubnik T, Volchenko N. Forecast of changes in the macroeconomic situation in Ukraine: smart economy of the future. Futurity Economics & Law. 2023;3(3):219-36.

17. oglu Macidov ST. Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations. Futurity Economics & Law. 2023;3(3):80-95.

18. Shakun N. Anthropological dilemmas of information society development modern stage in the context of globalisation challenges. Futurity Philosophy. 2022;1(3):52-63.

19. Nikolenko K. Artificial Intelligence and Society: Pros and Cons of the Present, Future Prospects. Futurity Philosophy. 2022;1(2):54-67.

20. Iliev K. Philosophical views on the procedure for regulating the norms of Blockchain technologies in the context of future prospects for the development of the meta-universe. Futurity Philosophy. 2022;1(1):30-41.

21. Maraieva U. On the formation of a new information worldview of the future (literature review). Futurity Philosophy. 2022;1(1):18-29.

22. Katerynych P. Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors). Communication & Society. 2022;35(4):37-53.

23. Kuryliuk Y, Filippov S, Kushnir I, Shvedova H, Berizko V. Subjects of the right to information on one's health in private and public law. Systematic Reviews in Pharmacy. 2020;11(10):827-31.

24. Kaplina O. Prisoner of war: Special status in the criminal proceedings of Ukraine and the right to exchange. Access to Just E Eur. 2022:8.

25. Muliarevych O, editor The Serverless Computing for Acceptance and Shipping Warehouse Zones Optimization. IT&I Workshops; 2022.

26. Rakhimov T, Mukhamediev M. Implementation of digital technologies in the medicine of the future. Futurity Medicine. 2022;1(2):14-25

27. Gushchyn O, Kotliarenko O, Panchenko I, Rezvorovych K. Cyberlaw in Ukraine: current status and future development. Futurity Economics & Law. 2022;2(1):4-11.

28. Lazareva A, Myroshnychenko V, Sanakuiev M, Gontarenko L. Philosophical discourse of information ethics of the future. Futurity Philosophy. 2023;2(1):14-29.

29. Dervīş L. Transformation of geopolitical perceptions in the Russian-Ukrainian war: impact on regional relations in the future. Futurity of Social Sciences. 2023;1(1):21-34.

30. Kalmykova O. Ukraine, Russia, and International Law: Occupation, Armed Conflict and Human Rights. Law, Business and Sustainability Herald. 2022;2(2):4-10.

31. Semenets-Orlova I., Mykhailych O., Klochko A., Nestulya S., Omelyanenko V. Readiness of the education manager to provide the organizational development of institutions (based on the sociological research). Problems and Perspectives in Management. 2019;17(3):132-142.

32. Semenets-Orlova I., Halytska N., Klochko A., Skakalska I., Kosyuk N. Information exchange and communication infrastructure in the public sector, CEUR Workshop Proceedings, International Workshop on Conflict Manage ment in Global Information Networks, CMiGIN 2019, Vol. 2588. Lviv, 2019.

33. Masyk M, Buryk Z, Radchenko O, Saienko V, Dziurakh Y. Criteria for governance'institutional effectiveness and quality in the context of sustainable development tasks. International Journal for Quality Research. 2023;17(2).

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.

Data curation: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.

Formal analysis: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.

Research: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.

Methodology: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.

Project management: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.

Drafting - original draft: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.

Writing - proofreading and editing: Oleksandr Galushchenko, Inna Pidbereznykh, Oleksandr Piroh, Dmytro Khrapach, Oleksii Tolmachov.