NATIONAL SECURITY DISCOURSE

DOI: 10.46340/eppd.2024.11.1.4

DIGITAL TRANSFORMATION AND NATIONAL SECURITY ENSURING

Lyudmila Kormych[1], D.Sc. in History; Tetiana Krasnopolska[2], PhD in Political Science; Yuliia Zavhorodnia[3], PhD in Political Science

[1] *National University "Odesa Law Academy", Odesa, Ukraine*

[2] *National University "Odesa Law Academy", Odesa, Ukraine*

[3] *National University "Odesa Law Academy", Odesa, Ukraine*

Corresponding author: Tetiana Krasnopolska; email: krasnopolskaya@onua.edu.ua

Citation: Kormych, L., Krasnopolska, T. & Zavhorodnia, Yu. (2024). Digital Transformation and National Security Ensuring. *Evropsky Politicky a Pravni Diskurz*, *11*, *1*, 29-37. https://doi.org/10.46340/eppd.2024.11.1.4

Abstract

The article analyzes the essence and consequences of digital transformation in modern society for the national security system. It is shown that the digital transformation that takes place in modern conditions actively affects the area of national security. It is proved that, on the one hand, it acts as a contributing factor to national security, since it increases the efficiency of public administration, and, being the main driver of reforms in this field, transforms the public policy system, leads to an expansion of citizens' political participation, and therefore democratizes public life. Also, digitalization expands the possibilities of influencing officials and other ambassadors of the state on foreign public opinion through digital public diplomacy. Moreover, the introduction of digital technologies may increase the level of economic development of the state. On the other hand, digital transformation poses several new threats to national security, namely in the economic, social, and information space. It contributes to digital political isolation, the shift of political activity in the digital environment and the emergence of new virtual unconventional forms of political participation, the development of cyber threats and cyberattacks, etc.

It is substantiated that the formation of a comprehensive national security system in the conditions of digital transformation will contribute to overcoming the threats of digitalization, the key development vectors, which in Ukraine include economic, information, and cybersecurity. It is proved that using the tools of these forms of security will help overcome the negative effects of digitalization and reinforce its positive role in society.

It is well-founded that digitalization is a new progressive process in government activity, with challenges and threats developing in cyberspace. An important component for the development of digitalization in developing countries is low material and transaction costs.

Keywords: digitalization, digital transformation, national security, information security, cyber security, economic security, public diplomacy, digital diplomacy.

Introduction

Nowadays, digitalization is a megatrend of global development. Human life and all of its spheres are now encompassed by digital technologies. This concerns work, specialization, education, leisure, and

socialization in general. Digitalization and technologization are the main drivers of the progress of society. So far, the leading area of digitalization of social processes is the economy, now turned into a "digital economy"[1], which implies the existence of Internet commerce, Internet banking, and electronic payment systems. In recent studies, politics has started to be considered in the context of the impact of digital technologies. There are studies on the specifics of the use of digital technologies in political processes, communications, and public administration.

In Ukraine, digital transformation is one of the main priorities in modern conditions that has covered the main areas of modern society and has become a hallmark of modern social development. It leads to several consequences, both positive and negative. All of this creates the need to consider the harmful effects of such processes and use the strengths of digital transformation to ensure the state's national security.

Research methodology

The theoretical basis of this study consists of the works of foreign and domestic scholars devoted to considering the digitalization and digital transformation processes and their impact on national security. The issues of the national security theory have been addressed by: H. Spencer (concept of enterprise security); D. Kaufmann (concept of team security), E. Carter (concept of humanitarian security), and others. Among domestic authors, the national security analysis has been addressed by A. Kolodii (concept of a systemic approach to the analysis of national security), V. Lipkan (concept of comprehensive analysis of national security), G. Sytnik (concept of synergistic analysis of national security), and others. The issues of digitalization and its impact on socio-political processes in the world, determining the role of the state in the information society were considered by A. Bancroft, P. Wright, O. Bjerg, S. Greengard, J. Schwartz, and others. The influence of digitalization on public activity and the formation of "digital citizenship"[2] was studied by L. Jones, J. Drexel, J. Cohen, K. Mitchell, D. Solove, E. Schmidt, and others. According to the author of the digital citizenship concept, K. Mossberger, digital citizens include those who often use digital technology to obtain political information in the performance of their civic duties and to obtain economic benefits during employment (Mossberger, Tolbert & McNeal, 2007).

The methodological basis of the study is represented by system-structural and comparative methods.

Results

Scientists believe that society is gradually moving towards the online world in modern life (Jensen, Danziger, & Venkatesh, 2007). Digital platforms can provide greater inclusion and accessibility for wider political and social participation in different contexts. For example, in Ukraine, we now have a fairly wide range of various directions, where such platforms work, which "allows you to receive any kind of service – educational services (Buki, Coursera), logistics (Lardi Trans), sales and retail (OLX, Prom, Rozetka), courier services and provision of services (kabanchik.ua), finance (purchase of insurance through Privat24), public procurement (Prozorro)" (Koleshnia, 2021).

According to M. Kaigo, the use of social media by civil society institutions expands political advocacy opportunities, connects with local government, and provides more opportunities for presence (Kaigo, 2017). In fact, a "hybrid model" is already being formed, using the Internet to ensure greater government transparency and the participation of citizens in decision-making. In addition, the feedback is strengthened. Thus, public politicians and political leaders and high-ranking officials, thanks to the use of the Internet, influence the general public not only in their country, but also abroad through the tools of "public diplomacy"[3]

[1] Economic activity that is ensured by the use of digital technologies, including IT developments and scientific digital solutions, e-commerce, online services and the results of activities of digitalized enterprises.

[2] A way of behaving, a set of norms and responsibilities that people should take into account when using digital technologies. These are all elements of digital life, from online safety to the right type of digital communication and responsible use of social media. It helps build the knowledge needed to participate in different communities (social networks or online discussion groups), as well as a critical understanding of which ones we want to join.

[3] Activities of high-ranking officials or other representatives of the state aimed at influencing public opinion in other countries and informing them further. Among other things, public diplomacy aims to create a positive image of the country in the eyes of the foreign public.

and "digital diplomacy"[1]. Digital public diplomacy is implemented using the following methods: placing radio and television broadcasts on the Internet; dissemination of literature in digital format; monitoring discussions in the blog space of foreign countries; creation of personalized pages of government members in social networks.

Digital communications increase the importance of citizen participation in public life. The Internet is becoming the second place of action for people. At the same time, the integration of cyberspace with real space takes place (Kellerman, 2014). K. Schwab, speaking about the Fourth Industrial Revolution and digitalization, notes: "Nowadays, the combination of computers, software, and networks… is so complex and integrated that it is already capable of transforming societies and the global economy," the author believes that the emergence of technologies beyond matter and penetration into other processes leads to "mixing… and interaction of physical, digital and biological spaces" (Schwab, 2016, p. 7-8).

It is worth noting that the term "digital transformation" itself was introduced into scientific vocabulary in the late 20th – early 21st centuries along with the use of the "automation", "computerization", "informatization", "digitalization" terms. Scientists understand this term as megatrends in the development of the economy based on cybernetic methods and management tools, artificial intelligence and big data analysis tools, which result in reaching a critical point in the digitalization of any business process or enterprise as a whole. At the same time, the transformation involves the process of a radical change in the form and mechanisms of functioning of the object or its elements under the influence of internal or external factors. The term "digitalization" was introduced into scientific vocabulary in 1995 by N. Negroponte, who compared atoms and bits, saying that just as in the material world everything consists of atoms, so in digital space, everything consists of bits (Negroponte, 1995).

The "digitalization" concept is considered in a narrow and broad sense. The first case is about the digitization of data, the transition from analog to digital format of accumulation, processing, and storage of information.

The second scenario envisions a shift in society and the economy driven by the widespread adoption of digital technologies. This transformation involves converting information into digital data, resulting in a more efficient economy and an enhanced quality of life for individuals. It is important to know the difference between the processes of informatization and digitalization. If the former involved the use of computer and information technologies to solve individual problems, the latter means the creation of a holistic environment for solving entire classes of problems.

Digital technologies have provided tools available to every individual to express any preferences, characterized by the lowest material and transaction costs. A feature of the digitalization of the political sphere is that the state and society are moving into a new communication environment, such phenomena as "Twitter revolutions"[2] and "Twitter diplomacy"[3] arise. The former is a factor of threats to national security, the latter, on the contrary, is an instrument of the national security system. Thus, as can be seen, digital transformation has a significant influence on the national security system.

In modern conditions, digital transformation is turning into an instrument of ensuring national security and a threat to such security at the same time. Particularly, digital technologies serve as the main driver of the transformation and increase the efficiency of public administration. They are already used in many government organizations, although, according to M. Grimsley and A. Meehan, it is now necessary to understand how their use and development of effectiveness of such structures (Grimsley & Meehan, 2007). Digital technologies serve as the basis for creating an organizational and technological base to improve the effectiveness of information services and the system of public authorities. S. Avgerou believes that the use of digital technologies can significantly increase the transparency of decisions in the field of public administration, reduce corruption levels, increase the confidence of citizens by involving them in the decision-making process (Avgerou, 2008).

[1] The emergence of digital diplomacy is associated with the rapid growth of the role of social media in public life and their penetration into the sphere of politics and allows state and non-state actors to convey their position to a multi-million foreign audience in the shortest possible time with minimal costs, instantly receive a response from the public and flexibly react by changing the content of their diplomatic activity.

[2] These are protests, demarches, revolutions, the regulation of which occurs through popular social networks, including Twitter.

[3] A new type of diplomacy that is carried out using the Twitter social network by state leaders, diplomats, embassies, organizations, etc.

It is worth noting that digital technologies most often affect national security indirectly – due to the impact of the dynamics of socio-economic processes. Therefore, countries lagging in terms of digitalization face several threats to national security. Among them: catching up with the world economy, a decrease in the competitiveness of their campaigns (especially compared to multinational corporations), limiting the prospects for innovative development, and limited instruments for ensuring national security.

Nowadays, there is no universal opinion on the acceptable limits for the digitalization of democracy (that is, procedures for political participation) and the system of public administration. The new technologies of social and political interaction, especially the possibilities of the Internet, are radically changing the format of security threats. Particularly, such threats as damage to telecommunications systems, the impact on elections through special programs, the influence on election results or their disruption, on the public consciousness by spreading misinformation or dosed information are possible only at a certain level of technological development.

According to K. Petroniuk, "the maintenance of international peace and security is at the center of the activities of the United Nations, and above all of the Security Council, remains one of the main goals set forth in its Charter, which contains several tools to achieve this goal. To this end, it must take all measures to stimulate and prevent all causes that threaten international peace and security, and if they remain, to eliminate them" (Petroniuk, 2023, p. 58).

We can support the opinion of A. Pravniuk's about information security, because "information protection or, better said, ensuring security is no longer just a technological problem. Issues related to information, its protection, information security and confidentiality become one of the measures to protect state sovereignty. Information has become the most important asset needed by a person, the state and society in general. Ensuring information security and protection of information sovereignty, forming one's own protected information space is one of the main tasks of the country." (Pravniuk, 2023).

Digitalization threatens economic and social stability, as well as information security. Particularly, cryptocurrency is a threat to economic stability, since it is most often used for money laundering and tax evasion, has no physical form and therefore its emission cannot be controlled by banks or the state. The threat to social stability lies in the significant impact on the labor market. Therefore, digital transformation contributes to the so-called polarization and leaching of the middle class of workers while increasing employment in the outer strata. Moreover, it requires retraining of workers, and sometimes increasing unemployment (for instance, due to the use of robotics). The modern threats posed by digitalization include the growth of cyber threats that involve potentially criminal actions against the information system of the state.

The magnitude of digital threats is increasing, they lead to significant financial, reputational, and time costs. Therefore, in the Global Risks Report of the World Economic Forum (The Global Risks Report, 2023), global threats such as cybercrime and data theft are ranked eighth by importance in the rating. That is why the challenges associated with digital technologies are becoming the subject of close attention of foreign leaders who intend to solve socio-economic problems and reduce the risks of digitalization by developing and implementing security strategies in the digital space (Gruber, 2017).

It is worth noting that the state, society, and the individual are equally interested in ensuring national security. In the second half of the 20th century, there was a tendency in the activities of the United Nations to prioritize the interests of the individual and civil society in the national security area. A broad interpretation of security appeared in the UN Millennium Declaration of September 8, 2000. According to the experts, the logic here lies in the fact that national security arises atop personal security, as well as international and global security. Therefore, a universal multi-level complex arises, which includes the security of the individual, society, and state.

The search for a balance between the powers of specialized bodies to ensure the individual, society, and state security and the unacceptability of their interference into the private sphere is relevant for modern countries. The effective development of the information society in the 21st century is seen in the combination of the maximum use of the opportunities provided by digital technologies with the benefits for humans and secure information space, to a decisive extent created by the efforts of the state.

All of the aforementioned requires creating an integrated approach to national security in the digital transformation context, which, according to the authors of this paper, includes three main components: economic, information, and cybersecurity.

Let's consider them in more detail. Thus, the main economic security problems include the problems of "digital inequality", lack of its element base, changes in the labor market, industrial espionage, personal data manipulation, and others.

The tools for solving the digital society problems include digital platforms for the development of the "sharing economy"[1], as well as "cloud" technologies and methods of processing major databases. The tool for monitoring the development of a networked digital society is the network readiness index (Network Readiness Index, 2023).

The information security system, in turn, requires strengthening and attracting more funds to ensure it. The state bears a responsibility to citizens for creating a secure information environment.

From the perspective of the practical component in the information environment, a set of threats has already been outlined, counteraction which is a key task of the state. In Ukraine, they are divided into external (the conduct of special information operations by the aggressor state against Ukraine, both on its territory and outside its borders; information expansion and information dominance of the aggressor state) and internal (insufficient development of the national information infrastructure; ineffectiveness of the state information policy; the imperfection of the legislation; the uncertainty of the strategic narrative; the insufficient level of the media culture of the society; the spread of calls for radical actions, the promotion of isolationist and autonomist concepts of the coexistence of regions in Ukraine) (Shevchuk, 2020, p. 291).

Consequently, information security is becoming one of the leading national security vectors. According to the legislation, Ukraine's information security is an integral part of the country's national security, the state of protection of crucial interests of an individual, society, and the state, in which an effective system of protection and counteraction to harm is established through the spread of negative information impacts, particularly coordinated dissemination of false information, negative consequences use of information technologies, unauthorized distribution, use, and violation of the integrity, confidentiality, and availability of information (Verkhovna Rada of Ukraine, 2021a).

The following political and legal acts are aimed at ensuring information security in Ukraine: National Security Strategy of Ukraine "Human Security – State Security" in 2020 (Verkhovna Rada of Ukraine, 2020), Cyber Security Strategy of Ukraine "Safe Cyberspace – the key to successful development" in 2021 and Information Security Strategy of Ukraine until 2025 (Verkhovna Rada of Ukraine, 2021b), adopted by the government and the National Security and Defense Council at the end of 2021.

In the context of digital transformation of information security includes the solution of the following tasks: identification of threats to information security; prevention of information leakage; monitoring and analysis of the information space; ensuring the unity, stability, and security of the information and telecommunications infrastructure of the state; integrated use of methods and means of computer systems protection in order to neutralize information security threats.

According to the Information Security Strategy of Ukraine until 2025, approved on September 15, 2021, by the Government and October 15, 2021, by the National Security and Defense Council, deterrence, stability, and cooperation are the main areas of information security in Ukraine. The Strategy identifies eight main objectives: countering misinformation, manipulative information, as well as foreign countries' information operations and attacks; ensuring the comprehensive development of Ukrainian culture and the establishment of national identity; raising the society's level of media culture and media literacy; ensuring respect for the constitutional human rights to freedom of expression and protection of privacy, protection of the rights of journalists, counteracting the spread of illegal content; informational reintegration of the residents of the temporarily annexed territories into the all-Ukrainian information space; creation and further development of the system of crisis communications; development and approval of a positive image of Ukraine and Ukrainians, information assistance to the promotion of the interests of the state in the world; development of the information society and increasing the level of the dialogue culture (Verkhovna Rada of Ukraine, 2021a).

It should be noted that the government has significantly intensified the implementation of the third goal of the Strategy. Particularly, the Unified State Portal of Digital Education was created (https://osvita.diia.gov.ua), and November of 2021 was declared the digital literacy month by the Ministry of Digital Transformation.

According to scientists, one of the promising ways to protect information is cryptography, which technologies allow identification and authentication objects and subjects of information networks; exercise control/limitation of access to information resources; guarantee the integrity of databases (Ivanov & Pysarenko, 2018).

[1] The sharing economy is a socio-economic system of acquiring, providing, or sharing access to goods and services, often facilitated by a website platform.

In modern conditions of digital transformation of public relations and public administration, the high incidence of cyber-attacks is becoming an acute problem for Ukraine, as well as for many other states. Therefore, ensuring cybersecurity is an important task of the state, which should be understood as the state of safety of public and private interests from illegal attacks carried out on computers, computer systems, and networks, as well as critical infrastructure objects. At the same time, the main problem is to establish the boundaries of state interference in those fields of information and communication systems that may become the object of cyberattacks.

The priorities of ensuring cyber security of Ukraine include the security of cyberspace to protect the sovereignty of the state and the development of society; protection of rights, freedoms, and legitimate interests of Ukrainian citizens in cyberspace; European and Euro-Atlantic integration in the area of cybersecurity (Verkhovna Rada of Ukraine, 2021a).

As co-authors Miguel Alberto Gómez and Christopher White successfully note "The growing importance of cyberspace as an instrument of national power requires a rigorous understanding of how preferences emerge in response to strategic developments within this domain. While schemas have become a mainstay over the past half-century, and although skepticism continues to abound regarding the analytic value of strategic culture, these should not deter researchers from employing these tools to better understand state behavior in this human-made domain" (Gomez & Whyte, 2022).

The security of digital systems is one of the critical "end-to-end" fields of digitization management, which requires adequate measures to protect all actors both within the country and at the global level, as digital threats and risks go beyond individual states and become global. In Western countries, the digital security strategy is often seen as a holistic document related to national security. In addition, national and international specialized organizations are being set up to coordinate network and information security. The main goals of the strategy of security in the digital space, researchers include detection of cyberattacks and response to them; prevention of threats, support, and development of reliable products and services for government agencies and economic entities; support for government agencies and infrastructure operators; promoting digital education (Van Caenegem & Skordas, 2007).

According to statistics provided by K. Sichkarenko, as of 2018, there were "the following ways of monetizing online education projects: sale of a program from a set of courses (Uniweb, Eduson) – on average $ 200-500 for each; sale of a video (Besmart) – up to $10 on average; course sale (Web.University, Udemy) – up to $100 on average; sale of subscriptions for the period (Netology, YaClass, LinguaLeo) – $ 20-25 per month; sale of certificates with a free course (Coursera) – $50-80 on average; sale of additional services – consultations, checking tasks, etc. (Earlydays) – on average $ 100-300; sale of visitor data to advertisers for targeted advertising (ResearchGate); processing of analytics on uploaded content and selection of necessary research for a separate fee (Academia.edu); provision of additional paid services, for example, storage of materials and organization of discussion platforms for universities (Mendeley); organization of an educational, recruiting and PR platform for the company (Udacity)" (Sichkarenko, 2018).

In general, it should be noted that, according to Ukrinform, "the number of cyberattacks on the Internet resources of authorities and media in Ukraine has tripled compared to last year". According to the State Service for Special Communications and Information Protection of Ukraine, in 2022, the State Center for Cyber Protection registered 2.8 times more cyber incidents than in 2021. The number of information security events in the categories "Malicious software code" and "Collection of information by an attacker" increased by 18.3 and 2.2 times, respectively. In 2023, the number of cyberattacks increased from 2022, by 15.9% to 2,543 incidents (In 2022 the number of … report, 2023).

According to Liga.net, "in three years, the number of cyberattacks in Ukraine has increased 5 times. Most of them are Russian" (Kondratova, 2022). In comparison: in 2021, Ukraine suffered 2,200 cyberattacks, in 2020 – 600, in 2019 – 480. In January 2022 – 121 cyberattacks (according to the SBU). So, the peculiarities of the development of cybercrime in the global world in: 2019 – 3.92 million dollars; 2020 – 3.86 million dollars; 2021 – 4.24 million dollars; 2022 – 1 trillion (Kormych & Zavhorodnia, 2023).

At the Ukrinform briefing in April 2022, Deputy Minister of Energy for Digital Development, Digital Transformations and Digitalization F. Safarov provided the following data on cyberattacks on the energy sector: "over the last 40 days of the war, the number of cyberattacks exceeded 200,000. For comparison, we had 900,000 attempts to attack infrastructure last year. In particular, about 20,000 attempts were recorded last week" (Pavlyshyn, 2022).

Developed countries are also developing national infrastructure protection programs that define technical and functional criteria for digital technologies and facilitate the identification of potentially

vulnerable elements through the development of rules and procedures for access to them. For example, Austria, Belgium, Portugal, Sweden, and the Czech Republic have set up emergency response teams to better exchange information and develop cooperation with private sector organizations, as well as to coordinate digital interaction between countries. Thus, the need for further international cooperation in the field of international and regional security in the digital environment is widely recognized.

Conclusions

In order to ensure information and cybersecurity, it is crucial to train specialists in this area. Particularly in Ukraine, over the past few years, higher education institutions started training specialists in the field of cybersecurity. With the dramatic increase in cybercrimes such as cyber-attacks, data fraud, stolen data features, etc. Cybersecurity has become one of the fastest-growing industries in the world. Therefore, there is a great demand for cybersecurity specialists.

Moreover, it is important to educate the population on the means of information safety, as well as to improve the media literacy of society. This is what the Unified State Portal of Digital Education of Ukraine (https://osvita.diia.gov.ua) is set to do. Mechanisms for the development of skills in the digital technologies field are part of the development of human capital and in the digital economy consist of three components: identifying the basic skills needed in the digital economy; forecasting changes in the economy as a whole and the labor market and assessing the ability of the education system to adapt to new conditions; use of digital technologies to improve the access and quality of education, for instance via online courses, etc. And this provided ample opportunities not only for education, but also for additional earnings.

Strengthening national security using digital technologies can be facilitated by the establishment of "digital citizenship", which implies a high level of readiness for the responsible, safe and effective use of digital communications. The fields of using the culture of digital citizenship are security, democracy, and business.

Today in Ukraine we have an active transition to acquiring knowledge specifically on online platforms, by taking various courses. The Ministry of Digital Transformation has launched a national online platform for digital literacy "Diia. Digital education", which is available on the Internet at the link: osvita.diia.gov.ua. On the online platform, every citizen can learn digital skills for free in a new modern format – an educational series.

Therefore, the study has shown that the digital transformation that is taking place in the current conditions is actively affecting the field of national security. On the one hand, it acts as a contributing factor to ensuring national security, since it increases the efficiency of public administration and is a major reform driver in this area, transforms the public policy system, expands political participation, and consequently democratizes public life. Furthermore, the introduction of digital technologies can increase the level of economic development of the country. However, on the other hand, digital transformation poses several new threats to national security, namely in the economic, social, and information space. Yes, it contributes to digital political isolation, the shift of political activity to the digital environment and the emergence of new virtual unconventional forms of political participation, the development of cyber threats and cyberattacks, and so on.

Overcoming the threats of digitalization will be facilitated by the formation of an integrated system of national security in the context of digital transformation, the key vectors of development of which in Ukraine include economic, information, and cyber security. Using the tools of these security forms will lead to overcoming the negative effects of digitalization and strengthening its positive role in society.

Acknowledgements. None.

Conflict of Interest. None.

References:

10+ naykrashchykh prohram dlya upravlinnya komandamy v 2021 rotsi (TOP vybirkovykh instrumentiv) [10+ Best Team Management Software in 2021 (TOP Pick Tools)] (2021). *Myservername.Com* https://uk.myservername.com/10-best-team-management-software-2021 [in Ukrainian].

Ahmed, E.M. (2017). ICT and Human Capital Spillover Effects in Achieving Sustainable East Asian Knowledge-Based Economies. *Journal of Knowledge Economy*, *8(3)*, 1086-1112. https://doi.org/10.1007/s13132-016-0430-4

Avgerou, C. (2008). Information Systems in Developing Countries: a Critical Research Review. *Journal of Information Technologies*, *23*, 133-144. https://doi.org/10.1057/palgrave.jit.2000136

Gomez M. A., Whyte, C. (2022). Unpacking Strategic Behavior in Cyberspace: a Schema-driven Approach. *Journal of Cybersecurity, 8(1)*. https://doi.org/10.1093/cybsec/tyac005

Grimsley, M., Meehan, A. (2007). E-Government Information Systems: Evaluation-led Design for Public Value and Client Trust. *European Journal of Information Systems, 16*, 134-149. https://doi.org/10.1057/palgrave.ejis.3000674

Gruber, H. (2017). Innovation, Skills and Investment: A Digital Industrial Policy for Europe. *Journal of Industrial and Business Economics, 44(3)*, 327-342 https://www.econstor.eu/handle/10419/169464

Ivanov, R.I., Pysarenko, L.D. (2018). Vykorystannia kryptohrafichnykh metodiv dlia zakhystu danykhu PK [Using Cryptographic Methods to Protect PC Data]. *Perspektyvni napriamky suchasnoi elektroniky»: materialy XII-yi naukovo-praktychnoi konferentsii (m. Kyiv, 19-20 kvitnia 2018 r.)* [Prospective Directions of Modern Electronics": Materials of the 12th Scientific and Practical Conference (Kyiv, April 19-20, 2018)]. Kyiv: KPI im. Ihoria Sikorskoho, 65-69 https://ed.kpi.ua/wp-content/uploads/conferences/2018/2018-Matherial_conferecne.pdf [in Ukrainian].

Jensen, M., Danziger, J. &Venkatesh, A. (2007). Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics. *Information Society, 23(1)*, 39-50. http://doi.org/10.1080/01972240601057528

Jones, L.M., Mitchell, K.J. (2016). Defining and Measuring Youth Digital Citizenship. *New Media & Society, 18(9)*, 2063-2079. https://doi.org/10.1177/1461444815577797

Kaigo, M. (2017). The Necessity of Digital Citizenship and Participation Information. *Information (Switzerland), 8(1)*, 28. https://doi.org/10.3390/info8010028

Kellerman, A. (2014). *The Internet as Second Action Space. Geographic Interpretations of the Internet. Springer Briefs in Geography.* Springer, Champ. https://doi.org/10.1007/978-3-319-33804-0

Koleshnya, Ya.O. (2021). Cyfrovi platformy yak efektyvna biznes-model [Digital Platforms as an Effective Business Model]. *Biznes, innovaciyi, menedzhment: problemy ta perspektyvy: mateiraly II Mizhnarodnoyi naukovo-praktychnoyi konferenciyi* [Business, Innovations, Management: Problems and Prospects: Materials of the II International Scientific and Practical Conference "Business, Innovations, Management: Problems and Prospects"], 80-81 http://confmanagement.kpi.ua/proc/article/view/230472 [in Ukrainian].

Kondratova, F. (2022). Za masshtabamy atak – ce Rosiya. Vnutrishnij front yak Kreml rozkhytuye Ukrayinu [In Terms of the Scale of the Attacks, it is Russia. The Domestic Front how the Kremlin Shakes Ukraine]. *Novyny Ukrayiny, Polityka. LIGA.net* [News of Ukraine, Policy. LIGA.net] https://www.liga.net/ua/politics/articles/po-masshtabam-atak-eto-rossiya-vnutrenniy-front-kak-kreml-raskachivaet-ukrainu [in Ukrainian].

Kormych, L., Zavhorodnia, Yu. (2023). The Concept of Modern Political Confrontation in Cyber Space. *Journal of Cybersecurity, 9(1)*. https://doi.org/10.1093/cybsec/tyad017

Lutska miska rada. Ofitsiinyi sait [Lutsk City Council. Official site] (2020). *V Ukraini realizovuietsia natsionalna onlain-platforma z tsyfrovoi hramotnosti "Diia. Tsyfrova osvita"* [In Ukraine, the national online platform for digital literacy "Action. Digital education"] https://www.lutskrada.gov.ua/publications/v-ukraini-realizovuietsia-natsionalna-onlain-platforma-z-tsyfrovoi-hramotnosti-diia-tsyfrova-osvita [in Ukrainian].

Mercer.Com (2023). *The Global Risks Report.* https://www.mercer.com/en-ca/insights/people-strategy/people-risks-and-business-resilience/global-risks-report-2023/

Mossberger, K., Tolbert, C. J. & McNeal R. S. (2007). *Digital Citizenship: The Internet, Society, and Participation.* Cambridge, MA: MIT Press https://www.academia.edu/34710283/Digital_Citizenship_The_Internet_Society_and_Participation

Negroponte, N. (1995). *Being Digital.* New York: Knopf https://web.stanford.edu/class/sts175/NewFiles/Negroponte.%20Being%20Digital.pdf

Network Readiness Index (2023). *Benchmarking the Future of the Network Economy* https://networkreadinessindex.org

Pavlysh, O. (2022). Za 40 dniv kilkist kiberatak na energosferu perevyshhyla 200 tysyach [In 40 Days, the Number of Cyber Attacks on the Energy Sector Exceeded 200,000]. *Ekonomichna pravda* [Economic Truth] https://www.epravda.com.ua/news/2022/04/12/685642/ [in Ukrainian].

Petroniuk, K. (2023). Powers and main mechanisms of the un security council in maintaining international peace and security. *Evropský Politický a Právní Diskurz* [European Political and Law Discourse], *10(4)*, 59-67. https://doi.org/10.46340/eppd.2023.10.4.3

Pravdiuk, A. (2023). Information Security of Ukraine: Information Influence and Information Wars. *Evropský Politický a Právní Diskurz* [European Political and Law Discourse], *10(1)*, 111-121. https://doi.org/10.46340/eppd.2023.10.1.6

Schwab, K. (2016). *The Fourth Industrial Revolution*. Geneva: World Economic Forum https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Shemchuk, V.V. (2020). Zahrozy informatsiinii bezpetsi: problemy vyznachennia ta podolannia [Threats to Information Security: Problems of Definition and Overcoming]. *Ekspert: paradyhmy yurydychnykh nauk*

i derzhavnoho upravlinnia [Expert: Paradigms of Legal Sciences and Public Administration], *1(7)*, 285-296. https://doi.org/10.32689/2617-9660-2020-1(7)-285-296 [in Ukrainian].

Sichkarenko, K.O. (2018). Rozvytok tsyfrovykh osvitnikh platform ta poshyrennia tsyfrovykh kompetentsii v osviti [Development of global educational platforms and the spread of digital competences in education]. *Efektyvna ekonomika* [Effective economy], *12*. https://doi.org/10.32702/2307-2105-2018.12.115 [in Ukrainian].

State Service of Special Communications and Information Protection of Ukraine (2023). *Report: the number of recorded cyber incidents almost tripled in 2022.* https://cip.gov.ua/en/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

Ukrinform (2022, 20 April). *Kilkist kiberatak u porivnyanni z mynulym rokom zbilshylasya vtrychi* [The Number of Cyber Attacks has Tripled Compared to Last Year]. https://www.ukrinform.ua/rubric-technology/3462508-kilkist-kiberatak-u-porivnanni-z-minulim-rokom-zbilsilasa-vtrici.html [in Ukrainian].

Van Caenegem, B., Skordas, T. (2007). Community research activities in secure and trustworthy ICT infrastructures. *Telecommunication Systems*, *35(3-4)*, 89-97. https://doi.org/10.1007/s11235-007-9043-3

Verkhovna Rada of Ukraine (2020, 14 September). *Ukaz Strategiya nacionalnoyi bezpeky Ukrayiny Bezpeka lyudyny – bezpeka krayiny* (Prezydent Ukrayiny) [Decree The National Security Strategy of Ukraine Human Security – Country Security, 2020 (President of Ukraine)]. https://zakon.rada.gov.ua/laws/show/392/2020#n7 [in Ukrainian].

Verkhovna Rada of Ukraine (2021a, 26 August). *Ukaz Strategiya kiberbezpeky Ukrayiny Bezpechnyj kiberprostir – zaporuka uspishnogo rozvytku krayiny* (Prezydent Ukrayiny) [Decree The Cyber Security Strategy of Ukraine Safe Cyberspace is the Key to the Successful Development of the Country (President of Ukraine)]. https://zakon.rada.gov.ua/laws/show/447/2021#n7 [in Ukrainian].

Verkhovna Rada of Ukraine (2021b, 28 December). *Ukaz Stratehiia informatsiinoi bezpeky Ukrainy* (Prezydent Ukrayiny) [Decree Information Security Strategy of Ukraine (President of Ukraine)]. https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].