Історико-політичні проблеми сучасного світу: Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2022. – Т. 46. – С. 159-166
DOI: 10.31861/mhpi2022.46.159-166

Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi: Chernivtsi National University, 2022. – Volume. 46. – pp. 159-166
DOI: 10.31861/mhpi2022.46.159-166

УДК 321.7:316.462

© Nataliia Khoma [1]
© Maiia Nikolaieva [2]

Digital Authoritarianism: Concept, Features, Threats

The article examines the content, features and threats of digital authoritarianism. The topic of the research is the result of a change in the configuration of non-democratic political regimes, which actively apply the achievements of scientific and technical progress, digital technologies for the implementation of control and supervisory functions. Digital authoritarianism is interpreted as a new political trend that contains explicit and implicit threats to the future of democracy, which makes its study relevant. The problem was investigated with the help of the methods of neo-institutionalism and the comparative method. The main cases for analysis are China and Russia, since they are the most active in developing, implementing and exporting digital authoritarianism. The aim of the article is to clarify the content of digital authoritarianism, its features, and the consequences of its implementation. To achieve the goal, the task is set: to consider modern approaches to understanding digital authoritarianism in political science; find out how the control and supervisory function of the state is strengthened by means of digital technologies; characterize the activities of authoritarian states regarding the export and import of digital authoritarianism. It is noted that the implementation of the control and supervisory function by authoritarian states through the use of digital technologies and artificial intelligence allows governments to automate the monitoring and tracking of the opposition. Digital tools make it possible for authoritarian regimes to cover a wide network of people with surveillance, which is especially used during mass protests.

Keywords: non-democratic political regimes, digital technologies, digital authoritarianism, export of authoritarianism, digital rights and freedoms.

Цифровий авторитаризм: поняття, особливості, загрози

Стаття розкриває зміст, особливості та загрози цифрового авторитаризму. Тематика дослідження є результатом зміни конфігурації недемократичних політичних режимів, які активно використовують досягнення науково-технічного прогресу, цифрові технології для здійснення контрольно-наглядових функцій. Цифровий авторитаризм трактується як новітній тренд політики, який містить явні та приховані загрози для майбутнього демократії, що актуалізує його вивчення. Проблема досліджувалася за допомогою методів неоінституціоналізму та компаративного методу. Основними кейсами для аналізу є Китай та Росія, позаяк вони найактивніше розробляють, впроваджують та експортують цифровий авторитаризм. Метою статті є з'ясування змісту цифрового авторитаризму, його особливостей, наслідків реалізації. Для досягнення мети поставлено завдання: розглянути сучасні підходи до розуміння цифрового авторитаризму політичною науковою; з'ясувати, як посилюється контрольно-наглядова функція держави за допомогою цифрових технологій; охарактеризувати діяльність авторитарних держав щодо експорту та імпорту цифрового авторитаризму. Відзначено, що реалізація авторитарними державами контрольно-наглядової функції з використанням цифрових технологій, штучного інтелекту дозволяє урядам автоматизувати моніторинг і відстеження опозиції. Цифрові інструменти уможливлюють охоплення авторитарними режимами наглядом широкої мережі людей, що особливо використовується під час масових протестів.

[1] ScD in Political Science, Professor at the Department of Political Sciences and International Relations, Lviv Polytechnic National University, Ukraine, E-mail: nataliia.m.khoma@lpnu.ua; https://orcid.org/0000-0002-2507-5741.
[2] PhD in Political Science, Assistant Professor at the Department of Political Science, Odesa I.I. Mechnikov National University**,** Ukraine, E-mail: nikolaeva.mayya@onu.edu.ua; https://orcid.org/0000-0003-0056-0553.

Ключові слова: недемократичні політичні режими, цифрові технології, цифровий авторитаризм, експорт авторитаризму, цифрові права та свободи.

Formulation of the research problem and its significance. Classical political regimes have been rapidly transforming in recent decades, acquiring new forms, characteristics, and varieties. This is facilitated by a wide range of reasons, one of which is technological progress, the development of Internet communication. Various technological and communication innovations very quickly have begun to be used in politics, activities of the state apparatus, etc.

If at first technological progress was widely accepted in democratic states, then rather instantly undemocratic politicians began to consider the latest technologies as effective tools for increasing their influence and strengthening their stability. Therefore, at the intersection of information and communication progress and non-democratic regimes, digital authoritarianism is born. It has already demonstrated new opportunities for non-democratic governments, as well as new threats to the quality of democracy, human rights and freedoms. These processes require scientific study, which actualizes the research of digital authoritarianism as a new political trend that contains explicit and implicit threats to the future of democracy.

Analysis of recent research on the problem. In Ukrainian political science, the issue of digital authoritarianism was developed at the level of analysing the individual cases of state influence on the Internet, digital human rights, the implementation of state control by means of digital recording, etc. Scientific conceptualization of digital authoritarianism, analysis of its consequences, threats, etc. were not carried out. At the same time, in recent years, Western researchers have intensified the elucidation of the content, forms, and consequences of digital authoritarianism. One may highlight the studies of M. Anthony, T. Dragu, E. Frantz, N. Gauchan, A.R. Gohdes, S. Greitens, V.A. Iii, A. Kendall-Taylor, L. Khalil, J. Lassila, K.-F. Lee, Y. Lupu, A. Mare, A. Polyakova, A. Przeworski, E. Sinkkonen, J. Wright, and others.

Research methodology. The study of the topic of digital authoritarianism is based primarily on the method of neo-institutionalism. With its help, it is possible to reveal how the institutions of non-democratic states use digital tools to strengthen their resilience. The research also relies on the comparative method, which reveals how different authoritarian states use the tools of digital authoritarianism, as well as implement its export or import policy.

Formulation of the purpose and tasks of the article. The purpose of the article is to clarify the content of digital authoritarianism, its features, and the consequences of its implementation within modern states. In order to achieve this goal, the following tasks are set: 1) to consider modern approaches to understanding digital authoritarianism by political science; 2) to find out how the control and supervisory function of the state is strengthened with the help of digital technologies; 3) characterize the activities of authoritarian states regarding the export and import of digital authoritarianism.

Research results. At the beginning of the active implementation of digital technologies, the prevailing opinion was that the Internet would become an exclusively democratizing tool[3]. In 2010, United States Secretary of State H. Clinton, in a speech on Internet freedom, expressed an opinion that the development of communication technologies and the free flow of information would lead to greater freedom and democracy[4]. Simultaneously, the democratic community was dominated by the belief that the progress of digital technologies, the Internet, social networks, and artificial intelligence would certainly serve to assert freedom of speech, would cause the fall of dictatorial regimes, and spread democracy around the world.

However, at present, this approach is perceived as idealistic. Modern political processes emphasize that autocrats have access to technologies designed to empower each individual, but they use them for the opposite purposes. Achievements of the information and communication progress are nowadays used not only by liberal democracies, but concurrently they strengthen the stability of non-democratic regimes. It seems that non-democratic politicians benefit even more from the results of technological progress than democratic leaders. Due to the scientific and technological progress, surveillance of citizens, people, objects, etc. is a daily reality.

[3] Glenny, M. 2011. *DarkMarket: CyberThieves, CyberCops and You, back in the 1990s*. New York: Knopf.
[4] Clinton, H. R. 2010. *Remarks on Internet Freedom* (speech, Washington, DC, January 21, 2010). Available from: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm. [25 October 2022].

One of the characteristics that distinguishes neo-authoritarianism from classical authoritarianism is the active use of digital tools to control citizens, political and legal institutions and other subjects. The governments of authoritarian states actively and aggressively use the opportunities created by the information and communication progress. Digital tools are beginning to complement (or replace) the classic tools of control and supervision, which have been tested for a long time in non-democratic states.

Currently, digital authoritarianism has become an international problem. The latest technologies of authoritarian control spread through global networks, both through private and public channels[5]. In authoritarian states, there is a consensus that the survival of their regimes depends, in particular, on the ability to apply such technologies. Consequently, one of the characteristics of the newest non-democratic regimes is that they are increasingly acquiring a digital form.

Modern non-democratic states are progressing at different rates in the process of digitization. Some of them develop, test and export digital technologies themselves, while others can only import and implement them to control their citizens. The export of digital authoritarianism by the states that are technologically ready to offer their developments to interested non-democratic governments, creates ever greater threats to democratic principles and values on a global scale.

Digital authoritarianism has not yet received a unanimous conceptualization by scientists as a concept, characteristic or tool of the newest non-democratic regimes. In scientific literature, digital authoritarianism is most often considered as a practice of repression and government control over citizens in cyberspace in the form of privacy violation, dissemination of disinformation, content filtering, etc.[6] L. Khalil defines digital authoritarianism as "the use of technology by authoritarian governments not only to control, but to shape, the behaviour of its citizens via surveillance, repression, manipulation, censorship, and the provision of services in order to retain and expand political control"[7].

The present paper discusses digital authoritarianism as the use of digital information technologies by authoritarian regimes for surveillance, repression, manipulation of citizens, disinformation, etc. That is, the use of digital tools by the authorities is considered both in relation to citizens and their digital rights, and in relation to the Internet as a whole.

Among the states that develop, implement within their borders, and also export, digital authoritarianism, China is in the lead. Such states also include Russia, Saudi Arabia, and others. The governments of technologically advanced neo-authoritarian states are testing various tools of digital authoritarianism both on their own citizens and in other states to which such technologies are exported.

The problem is seen in the fact that the latest information and communication technologies have significantly expanded the list of state tools for repression and social control, deepening the problems of democracy and human rights. Digital technologies have made repression and control much more common, more effective, more efficient, and cheaper. If in democratic states digital technologies have provided governments with new tools to communicate with citizens, understand public sentiments, and adapt government policies, in non-democratic states the same tools have given governments unprecedented opportunities to stay in power thanks to the increased control. Digital technologies make repression and control much more effective and invisible.

The content of digital authoritarianism is determined by the legislation adopted in a particular state. It is the government that determines what content on the Internet is prohibited or generally closes a national segment of the Internet from the world. The tools of digital authoritarianism are: blocking access to the Internet; content censorship; persecution for statements in the virtual dimension; disinformation; disconnection of the Internet; cyberattacks; targeted tracking by means of social networks, artificial intelligence; the use of facial recognition software, etc. Technologies such as artificial intelligence greatly expand the capabilities of the aforementioned tools of digital authoritarianism. At the same time, digital authoritarianism does not position itself as an authoritarian practice, but marks itself as, for example, a Smart City Initiative, a "crime control" mechanism, or other markers that are formally consistent with democracy and human rights.

[5] Dobson, W. J. 2012. *The Dictator's Learning Curve: Inside the Global Battle for Democracy*. New York: Random House.

[6]Anthony, M., Iii, V. A. & Gauchan, N. 2019. Dystopia is Now: Digital Authoritarianism and Human Rights in Asia. *Global Campus Human Rights Journal*, 3(2): 269-286; Mare, A. 2020. State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe. *International Journal of Communication*, 14: 4244-4263.

[7] Khalil, L. 2020. Digital Authoritarianism, China and COVID. Available from: https://www.lowyinstitute.org/publications/digital-authoritarianism-china-covid. [12 October 2022].

Global threats of digital authoritarianism are already evident. They no longer apply exclusively to large authoritarian states (China, Russia). Digital control and repression are recorded in most African states and in a significant part of Latin American states, in the Middle East and other regions of the planet. Currently, authoritarian states have intensified cooperation with digital exporting states to gain greater access to digital technologies. This interest of autocratic governments in digital technologies is due to the fact that they enable controlling the society more quickly, on a larger scale, and at lower costs. Consequently, authoritarian regimes that resort to digital repression strengthen their stability[8].

Advances in digital technology allow governments to control and track opponents of the regime[9]. This enables authoritarian governments to act proactively, to suppress organized opposition at its source. The impact of such processes on human rights is of concern. Internet technologies have become a new tool in the hands of authoritarian governments. Therefore, the pressure on the opposition and the critical part of society occurs both in real and virtual dimensions. "Cyber-utopia has now turned into cyber-dystopia"[10].

The methods used by digital authoritarianism were assessed as "preventive repression"[11]. Governments resort to such measures to reduce potential threats from the activities of the opposition and critical public. Preventive repression can include a wide range of tactics aimed at preventing, identifying, monitoring and tracking potential regime opponents in order to neutralize them before they pose a real threat to the current authorities. That is, under the conditions of digital authoritarianism, the focus of the state's attention has shifted: it tries not only to react to the actions of the opposition (the so-called "reactive repression"), but also to hamper its mobilization, to prevent its plans due to the monitoring of the digital space ("preventive repression"). This is done through censorship, monitoring of information flows, etc.

The tactics of different states vary depending on their economic and technological capabilities. Obviously, the opportunities of, for example, China and Turkmenistan are not the same. However, as current political processes demonstrate, governments of autocrats with even small technological and economic resources are capable of significantly undermining democracy and human rights. Authoritarian governments that exercise digital control have greater prospects for staying in power compared to governments that have not created sufficient material and technical prerequisites for this.

Behind the idea of strengthening the regulation of virtual space is the desire of the authorities to censor information, to control the public and private dimensions of the life of citizens, to prevent any possible threats to the stability of the current regime. These processes were caused by the emergence of new (digital) forms of discussion of social and political problems, which pose a threat to non-democratic regimes, given the speed of organizing anti-government actions. These processes were started by Twitter revolutions and Facebook revolutions, which originated from the so-called Brick Revolution (Moldova, April 2009). During the Arab Spring and subsequent protests and revolutions in different parts of the world, actions were coordinated through social networks. In fact, the number of various protests against authoritarian regimes has increased over the past two decades, and digital surveillance and prosecution for digital interactions have increased in response. The revolutionary "techno-optimism" of "the Arab Spring" period quickly gave way to the growth of digital authoritarianism. In countries where revolutions took place in the 2010s, and in the Middle East region in general, information and communication technologies were used "as a tool of counter-revolutionary repres-

[8] Kendall-Taylor, A., Frantz, E. & Wright, J. 2020. The Digital Dictators: How Technology Strengthens Autocracy. *Foreign Affairs*, 99(2), pp. 106, 112.

[9] Dickson, B. 2016. *The Dictator's Dilemma: The Chinese Communist Party's Strategy for Survival*. Oxford: Oxford University Press; Gohdes, A. R. 2020. Repression Technology: Internet Accessibility and State Violence. *American Journal of Political Science*, 64(3): 488-503; Milner, H. V. 2006. The Digital Divide the Role of Political Institutions in Technology Diffusion. *Comparative Political Studies*, 39(2): 176-199; Morozov, E. 2012. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs; Qin, B., Strömberg, D. &, Wu, Y. 2017. Why does China Allow Freer Social Media? Protests Versus Surveillance and Propaganda. *Journal of Economic Perspectives*, 31(1): 117-140.

[10] Wijayanto, W., Setiyono, B., Martini, R. & Nindya Elsitra, G. 2022. Digital Authoritarianism in Southeast Asia: A Systematic Literature Review. In: *Proceedings of the 6th International Conference on Social and Political Enquiries*, ICISPE 2021, 14-15 September 2021, Semarang, Indonesia. Available from: https://eudl.eu/pdf/10.4108/eai.14-9-2021.2321400 [6 October 2022].

[11] Dragu, T. & Przeworski, A. 2019. Preventive Repression: Two Types of Moral Hazard. *American Political Science Review*, 113(1): 77-87.

sion"[12]. The increased activity of Twitter bots greatly expanded the volume of disinformation, and networks of Internet trolls were deployed to intimidate opponents and hold important political debates.

Here is an example. Saudi Arabia has a network of pro-government bots and Internet trolls that generate more than 2,500 tweets daily[13]. An illustration of digital authoritarianism is the actions of the anti-Qatar coalition (Saudi Arabia, UAE, Egypt, Bahrain, etc.) in 2017 to justify the blockade of Qatar. Public relations companies, together with bots and Internet trolls, formed public opinion about the new "axis of evil" (Qatar, Turkey, the Muslim Brotherhood, etc.).

In order to enable the survival of authoritarian regimes, surveillance and pressure on the opposition and civil society were increased through digital means. The latest technologies allow governments to control opponents of an authoritarian regime, which can give them an advantage in putting pressure on opposition forces before they manage to pool their resources[14]. At the same time, the introduction of digital repression did not reduce the use of other, classical forms of pressure on the opposition, since digital tools of pressure and control are applied, first of all, to identify and control the opposition leaders as effectively as possible and, to a lesser extent, they can cover ordinary participants of mass protests.

Let us dwell in more detail on the issues of strengthening the control and supervisory function of the government over citizens with the help of digital technologies and the problem of export-import of digital authoritarianism.

Nowadays, digital technologies are actively applied by authoritarian states as a tool to strengthen the control and supervisory functions of authoritarian governments in relation to citizens, their associations and other actors. When it comes to digital authoritarianism, the case study of China needs to be investigated in the first place. The state has been investing in technologies designed to control the population for many years. This began in 1998 with the system of Internet censorship, web filtering, which was used for domestic control of web traffic ("Great Firewall", GFW). Without introducing full Internet censorship, the state limited the population's access to information from foreign sources.

The Chinese government has developed strict rules for users in terms of accessing websites whose content does not correspond to the official policy of the state. Most of the blocked sites are related to human rights, as well as movements for the independence of Taiwan and Tibet from China. Popular sites, platforms, instant messengers, search engines are also blocked: Google, YouTube, Meta, Twitter, Reddit, Blogspot, Bing, Wikipedia, LinkedIn, WhatsApp, Viber, Pinterest, Zoom, sites of many international non-governmental organizations (UNICEF, WHO, etc.), websites of world media, news agencies (Reuters, BBC, The New York Times, The Guardian, TIME, etc.). Some Internet resources from the prohibited list are available on Hainan Island, but only for tourists (Twitter, Messenger, Facebook). This demonstrates the economic pragmatism of the Chinese authorities who aim to obtain profits from the resort, recreation and tourism industries of the national economy.

Since 2013, China has operated a real name registration system for mobile phone users. And at the end of 2019, a government decision was made, according to which when buying a new smartphone or SIM card, the users must scan their faces. Such legislative innovations of the authorities are part of a set of initiatives to ensure cyber security by making it more difficult to access the Internet in incognito mode.

The COVID-19 pandemic substantially accelerated digital authoritarianism in China (and not only there)[15]. The Chinese government together with private companies (Tencent, Alibaba, etc.) developed programs for determining the state of health by analogy with traffic light colours (traffic light rating system). This program captures the risk of a certain person to public safety, for example, an elevated body temperature. When using certain programmes, users were required to enter personal and health information, and the mobile application tracked their movements, contacts and even their body temperature. The programs provided the collected data to the police and other authorities. This is an example of how authoritarian governments can apply technological advances to monitor citizens. Cur-

[12] Jones, M.O. 2022. *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. Oxford: Oxford University Press.

[13] Reporters Without Borders. 2020. *RSF unveils 20/2020 list of press freedom's digital predators*. Available from: https://rsf.org/en/rsf-unveils-202020-list-press-freedom-s-digital-predators. [23 October 2022].

[14] Dragu, T. & Lupu, Y. 2021. Digital Authoritarianism and the Future of Human Rights. *International Organization*, 75(4): 991-1017.

[15] Greitens, S. 2020. Surveillance, Security and Liberal Democracy in the Post-COVID World. *International Organization*, 74(1): 169-190.

rently, even in public transport (metro) of Chinese cities, face scanning programs are being launched. For example, in the Zhengzhou subway, you can pay your fare with the help of a program that scans passengers' faces. Passengers are encouraged to use the technology to get through turnstiles faster. In general, Xi Jinping's regime acquired the ability to predict potential protests and adapted its political ideology to the age of "Big Data", using artificial intelligence for surveillance and censorship.

China, Russia and some other neo-authoritarian states not only use the latest technologies to control their own citizens, but also extend new surveillance methods to less developed authoritarian states[16]. It is referred to exporting software, facial recognition systems, etc. China's experience, particularly, in applying digital tools for domestic censorship and surveillance made it the prime provider of such services for illiberal regimes seeking to deploy their own surveillance systems. China develops innovations for highly technological social control of the state over its citizens. China's IT exports are constantly changing. Nowadays, these are expensive and high-technology products and services developed and manufactured by local companies (Huawei, HikVision, Yitu, etc.)[17]. China exports its tools and even legal standards of digital authoritarianism to more than 60 countries as part of the Belt and Road Initiative[18].

China does not consider information technologies exclusively from the point of view of economic development, but from the point of view of their role in the implementation of the foreign policy course. Xi Jinping's regime is aggressively promoting Chinese information technology in the global market as part of its Belt and Road Initiative. For China, the export of information technologies is not only a source of replenishing the state budget, but it also creates strategic levers of influence on the West[19], despite the fact that certain Western countries (primarily the USA) introduced sanctions against China's high-technology sector.

It is noteworthy that currently the world democratic community has not given a powerful response to the export processes of digital authoritarianism. If this issue remains without the proper attention of the democratic community, it will result in strengthening the repression in non-democratic states (primarily in the third world) due to the applied digital technologies. Obviously, it is the democratic world community that must respond to the rising digital authoritarianism. For example, firms providing services to authoritarian regimes must be subject to sanctions. The West should develop a democratic model of digital governance that can compete with authoritarian models of Chinese, Russian and other styles.

As for Russia, although this country is currently increasing investments in the development of the mass surveillance system, this process is slowed down by financial and technological problems, as well as sanctions imposed on this country. Compared to highly technological China, Russia does not have such a high level of control over the movement of digital information. Therefore, the main strength of the Russian authorities in controlling citizens is based on threats of punishment, physical pressure on their offline space, and not on complex digital surveillance[20]. Even while controlling the Internet in Russia, the authorities primarily resort to various repressive offline methods, for instance, opening criminal cases against IT businesses, prosecuting bloggers, classifying them as "foreign agents", etc.

In 2020, a law came into force in Russia on mandatory pre-installation of Russian software on smartphones, tablets, computers and smart TVs: Mail.ru Group applications, "Gosuslugi" (state services) Internet portal, the Marusya voice virtual assistant and the Mir payment system. Subsequently, the list of programs was expanded. For the sale of equipment without these applications, sellers face a fine equivalent to up to 2.8 thousand dollars. Also, in recent years, the Russian government, by means of administrative coercion, has accelerated the collection of citizens' biometric data for their remote

[16] Sinkkonen, E. & Lassila, J. 2022. Digital Authoritarianism and Technological Cooperation in Sino-Russian Relations: Common Goals and Diverging Standpoints. In S. Kirchberger, S. Sinjen & N. Wörmer (eds.), *Russia-China Relations Global Power Shift*, Cham: Springer, p. 165.

[17] Lee, K.-F. 2018. *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin Harcourt.

[18] Coleman, V. & Napolitano, J. 2022. Digital Human Rights Need a Single Home in U.S. Government. *Foreign Policy.* 14 Mar.

[19] Kliman, D. & Grace, A. 2018. Power Play: Addressing China's Belt and Road Strategy. Washington: Center for a New American, pp. 10-11.

[20] Polyakova, A. & Meserole, C. 2019. Exporting Digital Authoritarianism: The Russian and Chinese Models. *Democracy & Disorder policy brief*. Washington, D.C.: Brookings Institution.

identification (the Unified Biometric System database). If citizens have not provided their biometric data, they cannot remotely receive public services. Collecting such data has not only positives, but also risks. The authorities can use such data to track citizens. Currently, biometric data are collected and processed by facial recognition systems using video surveillance cameras. If they are compared with the data of the Unified Biometric System database, the interested structures can create a complete portrait of persons and their movement. Criminal structures show similar interest, too. Since personal data in Russia are not reliably protected, a "black" market for biometric data, information on the movement of citizens, etc. is formed.

In the context of digital authoritarianism, the issue of online voting in elections at various levels cannot be avoided. Under the conditions of the coronavirus, Russian politicians saw certain advantages for themselves in online voting. In particular, in 2021, 25,000 Russian voters tested the remote electronic voting system. Later, deputies from the ruling United Russia party submitted a draft law on remote electronic voting to the parliament. Since that time, the idea of remote electronic voting has been supported by the Russian authorities, lobbying for the maximum conducting of the 2024 presidential elections as electronic voting. This meets the needs of an authoritarian regime that uses formal democratic procedures but distorts them. Therefore, even though electronic voting promotes wider electoral participation of citizens, it complicates independent monitoring of elections, which gives the current regime ample opportunities to remain in power.

The Russian digital tools that are exported (even despite the sanctions) to other authoritarian states are comparatively cheaper and less highly technological. First of all, this is in reference to means of surveillance, facial and speech recognition, various systems of operative and investigative activities. Their effectiveness is tested in the course of suppressing opposition movements and weakening the values of liberal democracy outside of Russia. Digital disinformation tools are also exported. These are technologies of information influence, which are relatively cheap and can be easily applied by state and non-state entities. Such low-technology tools, due to their low cost, are of interest primarily to third world countries, whose governments do not have the opportunity to purchase expensive technologies offered by other states. There are well-known cases of Russian digital export to Brazil, Mexico, Pakistan, Thailand, Sri Lanka and other states.

Conclusions. At present, neo-authoritarian regimes are actively applying information and communication progress for various forms of surveillance and control over citizens, business, civil society, etc. Despite the expectations that information and communication technologies will exclusively serve the progress of humanity, they are directed by authoritarian political forces to achieve destructive and anti-democratic goals.

Digital authoritarianism is not inherent only in separate states that develop, implement, and export digital control technologies. Now it is already a global system that includes states with different parameters of development and political regimes. Digital authoritarianism was formed as a certain system of actors and interactions. Some states (China, Russia, Saudi Arabia, etc.) and their technological corporations play the role of active entities that produce technological solutions, as well as implement them at the national level and export them. Other authoritarian states act exclusively as consumers of digital technologies, testing them on their citizens.

The implementation by authoritarian states of a control and supervisory function using digital technologies and artificial intelligence allows governments to automate the monitoring and tracking of the opposition in much less obvious ways than in the case of traditional surveillance. Digital tools enable authoritarian regimes to cover a wider network of people with surveillance than through methods that are dependent on people (secret services, law enforcement agencies, networks of informants, etc.).

Authoritarian regimes of technologically advanced states use digital technologies in the following main areas: 1) organization of surveillance of citizens and their associations; 2) neutralization of opposition efforts; 3) use of the advantages of digitization for propaganda, popularization of the regime, certain values. Technological innovations provide authoritarian governments with a wide array of tools to carry out activities that in many cases run counter to democratic standards.

While criticizing individual states for digital authoritarianism, we must understand that elements of such control exist in liberal democracies as well. Not only autocrat politicians, but also the leaders of Western democracies voice the ideas of new restrictions on digital rights. This is because the global decline of democracy over the past two decades has coincided with the emergence of new technologies of information gathering, communication and surveillance.

References

1. Anthony, M., Iii, V. A. & Gauchan, N. 2019. Dystopia is Now: Digital Authoritarianism and Human Rights in Asia. *Global Campus Human Rights Journal*, 3(2): 269-286.

2. Clinton, H. R. 2010. *Remarks on Internet Freedom* (speech, Washington, DC, January 21, 2010). Available from: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm [25 October 2022].

3. Coleman, V. & Napolitano, J. 2022. Digital Human Rights Need a Single Home in U.S. Government. *Foreign Policy.* 14 Mar.

4. Dickson, B. 2016. *The Dictator's Dilemma: The Chinese Communist Party's Strategy for Survival*. Oxford: Oxford University Press.

5. Dobson, W. J. 2012. *The Dictator's Learning Curve: Inside the Global Battle for Democracy*. New York: Random House.

6. Dragu, T. & Lupu, Y. 2021. Digital Authoritarianism and the Future of Human Rights. *International Organization*, 75(4): 991-1017.

7. Dragu, T. & Przeworski, A. 2019. Preventive Repression: Two Types of Moral Hazard. *American Political Science Review*, 113(1): 77-87.

8. Glenny, M. 2011. *DarkMarket: CyberThieves, CyberCops and You, back in the 1990s*. New York: Knopf.

9. Gohdes, A. R. 2020. Repression Technology: Internet Accessibility and State Violence. *American Journal of Political Science*, 64(3): 488-503.

10. Greitens, S. 2020. Surveillance, Security and Liberal Democracy in the Post-COVID World. *International Organization*, 74(1): 169-190.

11. Jones, M. O. 2022. *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. Oxford: Oxford University Press.

12. Kendall-Taylor, A., Frantz, E. & Wright, J. 2020. The Digital Dictators: How Technology Strengthens Autocracy. *Foreign Affairs*, 99(2): 103-115.

13. Khalil, L. 2020. Digital Authoritarianism, China and COVID. Available from: https://www.lowyinstitute.org/publications/digital-authoritarianism- china- covid. [12 October 2022].

14. Kliman, D. & Grace, A. 2018. Power Play: Addressing China's Belt and Road Strategy. Washington: Center for a New American.

15. Lee, K.-F. 2018. *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin Harcourt.

16. Mare, A. 2020. State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe. *International Journal of Communication*, 14: 4244-4263.

17. Milner, H. V. 2006. The Digital Divide the Role of Political Institutions in Technology Diffusion. *Comparative Political Studies*, 39(2): 176-199.

18. Morozov, E. 2012. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.

19. Polyakova, A. & Meserole, C. 2019. Exporting Digital Authoritarianism: The Russian and Chinese Models. *Democracy & Disorder policy brief*. Washington, D.C.: Brookings Institution.

20. Qin, B., Strömberg, D. &, Wu, Y. 2017. Why does China Allow Freer Social Media? Protests Versus Surveillance and Propaganda. *Journal of Economic Perspectives*, 31(1): 117-140.

21. Reporters Without Borders. 2020. *RSF unveils 20/2020 list of press freedom's digital predators*. Available from: https://rsf.org/en/rsf-unveils-202020-list-press-freedom-s-digital-predators [23 October 2022].

22. Sinkkonen, E. & Lassila, J. 2022. Digital Authoritarianism and Technological Cooperation in Sino-Russian Relations: Common Goals and Diverging Standpoints. In S. Kirchberger, S. Sinjen & N. Wörmer (eds.), *Russia-China Relations Global Power Shift*, Cham: Springer, pp. 165-184.

23. Wijayanto, W., Setiyono, B., Martini, R. & Nindya Elsitra, G. 2022. Digital Authoritarianism in Southeast Asia: A Systematic Literature Review. In: *Proceedings of the 6th International Conference on Social and Political Enquiries*, ICISPE 2021, 14-15 September 2021, Semarang, Indonesia. Available from: https://eudl.eu/pdf/10.4108/eai.14-9-2021.2321400 [6 October 2022].