Journal of Political Science: Bulletin of Yerevan University
2023, VOL. 2, NO. 3 (6), December, 62-75
https://doi.org/10.46991/JOPS/2023.2.6.062

DIGITAL AUTHORITARIANISM AS A MODERN THREAT TO DEMOCRATIC STABILITY: RESTRICTION OF FREEDOM OR NETWORK POLITICIZATION?

ARMEN MIRZOYAN*
Yerevan State University

Abstract
This article is dedicated to the identification of contemporary instances of digital authoritarianism, exploring its definitions, characteristics, methodologies, and the tools employed by authoritarian governments to manipulate the social and political conduct of their citizens and control the flow of information. It aimed to consolidate power, control and manipulate information, and suppress dissent. The article delves into the various interpretations of digital authoritarianism by analyzing its fundamental elements and evident expressions. Through a comprehensive review of scholarly literature, reports, news publications and case studies, the article aims to unravel the dynamic nature of digital authoritarianism, shedding light on how it adjusts to technological progress and confronts conventional notions of liberty within the digital era. Digital authoritarianism materializes through mass surveillance, cyber attacks, information censorship, and the targeted utilization of citizen data. A thorough exploration of digital authoritarianism can empower democratic societies to preclude potential infiltration of such manifestations, uphold democratic principles, and arrange the landscape based on these principles while ensuring unfettered access to information.

Keywords: digital, authoritarianism, dictatorship, power, mass surveillance, regime, facial recognition, control, espionage, cyberattacks, censorship.

Introduction

The primary purpose of the study is to make a comprehensive analysis of the concept of 'digital authoritarianism', to understand if a universal definition exists, and to explore characteristics, methodologies, and the tools utilized by authoritarian regimes to influence the societal and political behavior of their populace, as well as its impact on the democratic order. No attempts have yet been made in the Armenian academic field to study the concept of 'digital authoritarianism', as well as its impact on the democratic

[*] **Armen Mirzoyan** is a PhD candidate of the Chair of Political Science at Yerevan State University. He is a Journalist for Hetq.am and Project Manager at "Investigative Journalists" NGO. Email: armen.mirzoyan@ysu.am. ORCID: https://orcid.org/0009-0008-2396-4933.

Received: 12.11.2023
Revised: 24.12.2023
Accepted: 04.12.2023

order. Thus this article aims to find out whether there is a single definition of digital authoritarianism, and what are the main tools that authoritarian regimes use to purposefully manage society and information flow.

Back in 2018, when the Freedom House, a human rights organization published the 'Freedom on the Net 2018' report, Adrian Shahbaz the vice president for Research and Analysis of the organization published an article that clearly emphasizes the rise of digital authoritarianism around the world. Based on the conducted research and data from previous years, Shahbaz claimed that "the internet is growing less free around the world, and democracy itself is withering under its influence" (Shahbaz 2018). At the very beginning of his article, Shahbaz emphasizes that disinformation and propaganda spread across the internet have contaminated the realm of public discourse.

The importance of digitalization for society and the political regime

Digitalization and digital transformation have recently received great attention both from representatives of states and from international organizations. Digital technologies can benefit society by facilitating access to government services, increasing employment and economic growth, which can contribute to improving the well-being of citizens. State-driven digitalization complements and compensates for traditional and formal mechanisms of interaction between citizens and government, creating additional online institutions. Moreover, digitalization has significantly changed the relationship between state and society, gradually increasing the frequency and quality of interaction between citizens and government.

The unrestrained gathering of individual information has eroded conventional concepts of personal privacy. Additionally, a group of nations is progressing towards digital authoritarianism by adopting the Chinese approach of widespread censorship and automated surveillance mechanisms. He added that for 8 years, starting in 2010, global internet freedom declined for the eighth consecutive year in 2018 (Shahbaz 2018; Richey 2018).

In 2022, despite expectations that global progress would lead to an increase in democracy and its expansion to non-democratic regions, the situation deteriorated further. Compared to 2018, the problems, challenges and threats not only remained the same but worsened even more. The COVID-19 pandemic occurred and Russia invaded Ukraine in February 2022, as a result of which the free press was practically eliminated in Russia, free expression of will against military actions became criminalized, deprived of liberty or thousands of dissidents and Russians opposed to the Kremlin's policy have left the country (Kravtsov 2022).

Moreover, Freedom House in its report "Freedom on the Net 2022" repeats the same phrase that Adrian Shahbaz wrote about back in 2018, just this time the number 8 was replaced by 12. Freedom House continues to claim that Global internet freedom declined for the 12th consecutive year. According to this organization, the sharpest downgrades were documented in Russia, Myanmar, Sudan and Libya and at least 53 countries, users faced legal repercussions for expressing themselves online, often leading to prison terms (Freedom House 2022, 8). According to Freedom House, in the world, over 4.5 billion people have access to the Internet, while 76% of them live in countries where individuals were arrested or imprisoned for posting content on political, social or religious issues. Even more, 69% live in countries where authorities deployed pro-government commentators to manipulate online discussions. Moreover, 64% live in countries where political, social or religious content was blocked online and 51% live in countries where access to social media platforms was temporarily or permanently restricted.

In the last two decades, when information technologies are rapidly developing, political processes are also being transformed and modernized in parallel with their development. Several political processes that have taken place over the past two decades, including election campaigns, debates, revolutions or military actions, are actively accompanied by the active use of modern technologies. A striking example of this was the Arab Spring, political changes in Armenia in 2018, the Russian invasion of Ukraine, etc. (Aleksanyan and Aleksanyan 2022).

Information technologies are also used to spread fake news and disinformation, the regulation of which is extremely difficult in democratic and transitional countries, since there may be a serious threat to the restriction of freedom of speech, but this does not mean that the field should be in a neglected state. Being well aware of the possibilities and means of controlling society through online media, social networks and modern information technologies, authoritarian regimes seek to take them into their own hands, restricting human rights and freedoms, as well as controlling any information flow that may harm the current regime (Aleksanyan 2022; Rothacher 2021).

Contemporary digital authoritarianism is often used in the scientific literature in the variants of digital dictatorship, techno-authoritarianism, or IT-backed authoritarianism, which shows that there is no single approach to the study of digital authoritarianism (Kravtsov 2022; Ellis 2022). Over the past two decades, the development of information technologies has led to changes in political science terminology.

Digital understanding of the legitimation of regime influences

Alina Polyakova and Chris Meserole digital authoritarianism define as the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations (Polyakova and Meserole 2019). Polyakova and Meserole note that digital authoritarianism is reshaping the power balance between democracies and autocracies. In their article published in Foreign Policy at Brookings, the authors consider the examples of China and Russia and note that China and Russia have created unique and technology-centered strategies for governing under authoritarian regimes, which they have also shared with other nations. "Beijing's experience using digital tools for domestic censorship and surveillance has made it the supplier of choice for illiberal regimes looking to deploy their own surveillance systems, while Moscow's lower-cost digital disinformation tools have proven effective in repressing potential opposition at home and undermining democracies abroad", says Polyakova and Meserole (Polyakova and Meserole 2019).

A similar definition is given by the analyst of the Lowy Institute, Deakin University researcher Lydia Khalil, according to which Digital authoritarianism is the use of technology by authoritarian governments not only to control, but to shape, the behavior of its citizens via surveillance, repression, manipulation, censorship, and the provision of services in order to retain and expand political control (Khalil 2020).

According to DW Akademie, which is the academic center of Deutsche Welle, Digital authoritarianism is mostly described as a way for governments to assert power and control information flows through digital tools and the Internet (Albrecht and Naithani 2022).

Erol Yayboke and Samuel Brannen, researchers from the Center for Strategic and International Studies (CSIS) in Washington, DC, define Digital authoritarianism as the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties (Yayboke and Brannen 2020). According to them, Digital authoritarianism appropriates and distorts the fundamental values of open and democratic societies. Its objective isn't solely to dismantle these principles, but to redefine and mold them according to its authoritarian model.

Categorizing digital authoritarianism within a nation's political structure is challenging. Instead, it encompasses a diverse array of approaches, tools, tactics, and technological measures that governments utilize to exert control and exert significant power over their populace. These methods and resources are increasingly undermining the progress of internet governance that prioritizes human rights. Additionally, they run counter to governments' obligations to safeguard individuals' rights to privacy, freedom of expression, and peaceful assembly (Krapiva and Zhyrmont 2023).

The Carnegie Endowment for International Peace in the Democracy, Conflict, and Governance Program's senior fellow Steven Feldstein in his 'The Global Expansion of AI Surveillance' report, which was published in September 2019, indicates that digital repression, which authoritarian regimes use, comprises six techniques: surveillance, censorship, social manipulation and harassment, cyberattacks, internet shutdowns and targeted persecution against online users (Feldstein 2019). According to him, these six techniques are not mutually exclusive. "Intrusive spyware, for example, implanted by government security services on a user's computer, is both a form of surveillance as well as a cyberattack. But each technique offers a specific set of objectives and draws from a unique set of tools in order to fulfill its function", says Feldstein.

Feldstein is among the researchers who are alleging that digital authoritarianism is being propagated not only by authoritarian governments like Russia and China, but also by several democratic nations such as the USA, Israel, United Kingdom, and France. This involves the creation of tools and software that significantly undermine human rights, democratic values, and political freedoms. Democratic countries also supply advanced capabilities to repressive regimes — from location-tracking spyware and hi-resolution video surveillance, to hacking software, and censorship filtering applications. Analysts who overstate China's role run the risk of oversimplifying a complex environment and ignoring other culpable actors who are supplying powerful capabilities to bad governments, writes Feldstein (Feldstein 2019, 8).

Information hegemony and digital sovereignty

Hybrid mechanisms for introducing digital technologies, similar to those in China, Russia and Kazakhstan, are emerging all over the world. A variety of political regimes are constantly looking for new ways to legitimize themselves through the formation of citizens' trust in their activities. The cardinal goal of various innovative legitimation practices is to create agreement between representatives of the political elite and civil society that the existing political regime is effective, fair and capable of solving complex problems.

Erol Yayboke and Samuel Brannen in their ‘Promote and Build: A Strategic Approach to Digital Authoritarianism’ report put forward four overlapping problems that democratic systems face and which further strengthen the position of digital security (Yayboke and Brannen 2020). According to them, the first is that digital authoritarianism is expanding within existing authoritarian-led states, like in China, Russia, Iran or Saudi Arabia. These countries spend huge sums on population control, information flow management, and artificial intelligence. Facial recognition has enhanced their capacity to monitor and manipulate the activities of individual citizens to a greater extent. The most striking example of this is the Social Credit System, a national credit rating and blacklist developed by the government of the People’s Republic of China.

The social credit project aims to create a system where the trustworthiness of businesses, individuals, and government entities is monitored and assessed through a record-keeping system. Various versions of the social credit system are being tested, with the primary national approach involving the utilization of blacklisting and whitelisting methods for regulation. Like Feldstein, Yaybroke and Brannen also draw attention to the issue of authoritarian regimes sharing the tools they employ with other regimes that do not oppose their usage. At the same time, as the researchers note, this is done not only to strengthen the connection between the regimes but also for commercial benefit.

As noted above, this practice is often used by democratic countries that sell various software and tools to authoritarian regimes. Israel is a fresh example of this: The Israeli NSO Group is the creator of the Pegasus, a famous spy program. Over the past few years, this software has been caught up in a number of political scandals (Mirzoyan 2021). It was used to eavesdrop on world leaders, journalists, representatives of civil society, and especially activists (BBC 2021). At the same time, the process of eavesdropping or the orders for it were mostly given by non-democratic regimes, including Azerbaijan.

On May 25, 2023, Amnesty International’s Security Lab, Access Now, The Citizen Lab, and CyberHUB.am published an investigation, according to which at least 12 people in Armenia were targeted by the Pegasus spy program in the period from October 2020 to December 2022 (Amnesty International 2023). The authors of the investigation, who are also IT security specialists, suggest that the Karabakh conflict could have caused such persecution, and Azerbaijan could become the customer. Experts claim that this is the first documented evidence of the use of the Pegasus spyware during military operations. According to Samvel Martirosyan, an Armenia media expert, during the hostilities, if the Pegasus spyware’s customer was Azerbaijan, it means that the Israeli government officially allowed that country to use cyberweapons against Armenia (Factor

TV 2023). According to Martirosyan, Karlen Aslanyan and Astghik Bedevyan, journalists of Radio Free Europe/Radio Liberty, former human rights defender Kristinne Grigoryan, turkologist Varuzhan Geghamyan, lawyer Ruben Melikyan, former MP from RPA Samvel Farmanyan, former press secretary of the Ministry of Foreign Affairs Anna Naghdalyan eavesdropped through Pegasus.

The next important challenge is that authoritarian regimes abroad are expanding access to their digital tools by spying and eavesdropping on their citizens and citizens of foreign countries. The same investigation by Amnesty International and other organizations notes that there were revealed more than 1,000 Azerbaijani phone numbers which were selected for targeting by a Pegasus customer. Some of these phone numbers belonged to journalists, including Khadija Ismayilova (JAM-news 2021), opposition politicians, from which researchers suggest that the Azerbaijani government may also be behind this, since, according to NSO Group, Pegasus is sold only to state bodies. In addition, the company claimed that the entity provides only technology, and its launch and data collection is carried out by the customer.

Lastly, these techniques or challenges used by digital authoritarianism might also find application in democratic nations by political parties, special interest organizations, or businesses driven by an anti-democratic set of principles that disregard public confidence, individual liberties, human rights, and other fundamental civil freedoms.

Erol Yayboke and Samuel Brannen in their ‘Promote and Build: A Strategic Approach to Digital Authoritarianism’ report highlight tools that are very characteristic of digital authoritarianism and are used by non-democratic regimes. These tools include surveillance, cyberattacks and espionage, censorship, social and electoral manipulation (Yayboke and Brannen 2020). Nonetheless, this doesn’t imply that democratic systems cannot utilize these techniques, albeit typically on a smaller scale and often for different intentions compared to how authoritarian governments employ them (Sinkkonen and Lassila 2022).

Each of these tools can be applicable to the challenges mentioned above, or be general. So, mass surveillance, which can be carried out using cameras, phones, Internet-connected equipment, GPS systems or other modern technologies, is perhaps the simplest and, as noted by Yayboke and Brannen, the most accessible. Contemporary advancements in technology enable us not just to comprehend the whereabouts and potential actions of these individuals, but also to gather and convey essential data. Intelligence agencies, including those in democratic nations, are involved in the acquisition of such information as well, and modern technologies offer ample possibilities to acquire the required data (Schatz 2023; Isaacs 2022).

Recently, the rising features of artificial intelligence have given even more opportunities for the modernization of mass surveillance technologies. For example, Xi Jinping has spearheaded the development of digital authoritarianism in China under the Chinese Communist Party (CCP). This strategy involves employing censorship, propaganda, and AI-powered population-wide surveillance. In 2017, China’s government unveiled an ambitious strategy to position itself as a prominent worldwide center for AI advancement by 2030. The government designated Baidu, Tencent, Alibaba, and iFLYTEK, a speech recognition software company, as the key players in the field of AI on a national level. As individuals’ lives progressively hinge on their technologies, these corporations have amassed significant sway. Ranging from smart voice assistants to sensors that gather data for analyzing living conditions, their inventive solutions aspire to elevate the overall quality of life (Roberts et al. 2021).

The Chinese population has grown accustomed to big tech companies and the state overseeing various aspects of their lives, including personal interests, education, health, academic qualifications, economic status, consumption habits, social interactions and even reading preferences. Utilizing an extensive network of cameras with facial recognition capabilities and a crowdsourced reporting system enables an unparalleled level of monitoring granularity and the potential for individual behavior manipulation. In 2019, data leaks revealed that Chinese authorities were closely tracking the locations of almost 2.6 million people in real time through a facial-recognition company and police contractor called SenseNets (Yang and Murgia 2019).

The problem is that the Chinese government has exported surveillance systems to more than 80 countries around the world, raising concerns about democratic backsliding and the rights of individuals there (Greitens 2020).

Erol Yayboke and Samuel Brannen indicate that surveillance is used for all four challenges. Authoritarian regimes often apply for cyber attacks and online espionage, which allows them to obtain sensitive information that can be valuable from a strategic and tactical point of view. Digital espionage encompasses a wide range of strategies, such as hacking, distributed denial-of-service (DDoS) attacks, phishing emails, spyware, malware, ransomware, and network intrusions. This form of espionage may be motivated by economic interests, as it involves stealing sensitive commercial data and intellectual property, which gives the private sector a competitive advantage.

Cambridge Dictionary defines cyberattacks as an illegal attempt to harm someone's computer system or the information on it, using the internet. Cyberattacks can be aimed not only at obtaining information but also at creating internal political confusion in a given country. A striking example of this was the cyberattack on the Democratic National Committee computer network in 2015 and 2016, which, according to the American government and cybersecurity experts, was backed by Russian hacker groups (Perez and Diaz 2017). As a result, hackers published personal correspondence, documents, and materials of the internal turnover of the Democratic Party. One of the scandalous publications concerned Hillary Clinton, who was the presidential candidate of the Democratic Party at that time. This was done in order to show that the former secretary of state during her office, instead of having an email in the @state.gov domain, the official correspondence conducted by her personal email, which caused a serious scandal around security and accountability in the United States.

Representatives of the Democratic Party and independent experts argued that this was how Russia interfered in the internal affairs of the United States, helping to elect the Republican candidate, billionaire Donald Trump, who was the most preferred candidate for Moscow.

Another well-known example of a disorder in another country's internal political sphere and influence on the electoral process is the attack on the emails of Emmanuel Macron and his campaign headquarters, which occurred in 2017, two days before the presidential elections in France. Unlike the American one, this leak, containing about 20,000 emails, did not affect the elections in France. One of the main reasons for this was that according to the Electoral code of this country, the Day of Silence in France lasts 44 hours, and the media, based on this, could not publish them. Macron and his political team accused Russia of the attack, claiming that by doing so Vladimir Putin was trying to support his most preferred candidate, the right-wing politician Marine Le Pen. Both in the case of the American attack and in the case of the French one, the Kremlin denied its involvement.

Independent experts claim that the Kremlin has also used cyber operations to disrupt organizations that are essential to the functioning of democracy, including legislatures (such as the German Bundestag and UK Parliament) and political parties (in Estonia, France, and Germany) (Brandt and Taussig 2019; Glazunova 2022).

Erol Yayboke and Samuel Brannen note that this tool is used in the frame of the second (sharing the tools they employ with other regimes) and third challenges (spying and eavesdropping on their citizens and citizens of foreign countries abroad).

The next tool is censorship, in this case, online censorship and Internet control. In authoritarian regimes, Internet control is generally explained by domestic power preservation: to curtail dissent within their borders, authoritarian regimes censor, monitor, and shape online communications (Michaelsen 2018; Sinkkonen and Lassila 2022). They use various methods to limit access to information, control the flow of data, and suppress dissenting voices to maintain their hold on power and control the narrative. Several tactics for censorship may include Internet filtering and blocking, content removal, surveillance and monitoring, online misinformation and propaganda, legal and regulatory measures, etc.

During critical political times, authoritarian regimes are compelling internet service providers to deliberately reduce or restrict their services, a practice known as ‘throttling’. This action encroaches upon the freedom of expression, obstructs journalists from disseminating crucial updates to the public, and hampers the unrestricted dissemination of information (Woodhams 2020).

The governments have also imposed challenging legal requirements on online platforms, compelling them to remove objectionable content. Another method is in China, where the government uses AI to screen video footage for images of objects like tanks and candles that could be associated with protest messages - a feat made possible by technology, as the video was previously difficult to monitor because it required too much manpower (Mozur 2021).

Modern countries with authoritarian regimes also create their own version of the Internet, for example, in North Korea with a totalitarian regime, the ordinary population does not have access to the Internet. This advantage is reserved for a group of people related to the ruling political elite of this country (Williams 2010). Instead, ordinary citizens can connect to the internal intranet system from libraries or other institutions, where the available information is filtered out by the North Korean authorities and presented in a way that benefits Pyongyang and the ruling Kim family (Yilmaz and Yang 2023).

China has gone the other way. As mentioned above, it has created local websites and applications that not only provide the authorities with the necessary information but are also directly related to people’s daily lives (Qiaoan and Teets 2020; Taylor 2022). For example, through WeChat Chinese people do social networking, including sending messages, and doing stories. Any government organization, company, or group can register a WeChat Official Account to send articles and messages to their followers, order in a restaurant, shop, pay, etc. (Zheng 2020).

Russia has also been developing the so-called ‘Runet’. The latter is a general term that defines the Russian and Russian-speaking parts of the entire Internet. Experts say that the Russian authorities are moving according to the Chinese scenario. They are trying to create Russian versions of the world's leading websites and platforms that will not only be under their own control but also independently of the West. These countries very often claim that they are going for digital sovereignty which gives the state greater political control over the use of the Internet in its jurisdiction.

Erol Yayboke and Samuel Brannen indicate that this tool is used in the first (digital authoritarianism is expanding within existing authoritarian-led states), second (sharing the tools they employ with other regimes) and fourth (digital authoritarianism might also find application in democratic nations by political parties, special interest organizations, or businesses driven by an anti-democratic set of principles) challenges.

The last tool is social and electoral manipulation. Non-democratic regimes use digital technologies and online platforms to control, influence, and manipulate public opinion, suppress dissent, and shape electoral outcomes. In this process, they use Social Media bots, Troll farms, Fake News, Social Media Advertising, Content Amplification Networks, disinformation campaigns, etc. For example, social media bots create and spread pro-regime narratives. These bots mimic human behaviour on social media by engaging in activities such as commenting, liking, posting, and sharing content. They give the illusion of being real users, but in reality, they are automated programs designed to interact and behave like humans.

“Many governments are finding that on social media, propaganda works better than censorship. Authoritarians and populists around the globe are exploiting both human nature and computer algorithms to conquer the ballot box, running roughshod over rules designed to ensure free and fair elections”, said Mike Abramowitz, President of Freedom House (Freedom House 2019). Besides that, authoritarian governments target the computers and mobile devices, as well as social media and email accounts, of civil society leaders, seeking access to confidential communications and contacts.

The most difficult scientific problem seems, first of all, to determine the deep transformations of social and political reality under the pressure of accelerated digitalization. Meanwhile, before the pandemic itself, the prerequisites for the transformation of traditional political processes and institutions had already been created. The reason for this was the emergence of new economic players and global digital companies (Google, IBM, Apple, Microsoft, Alibaba and others), which gave rise to digital platforms, algorithms and various network effects that subjugate the very communication channels of citizens and force, in turn, to reconsider the traditional concept sovereignty (Gosztonyi 2023; Yilmaz 2023).

Authoritarian governments employ computer programs capable of accessing, sorting, and analyzing vast amounts of gathered data to analyze information. Among the commercially available software used for this purpose are SolarWinds, NetFlow, Traffic Analyzer, etc. (Schlumberger et al. 2023).

Conclusion and discussion

Modern digitalization actualizes other problems associated with the risk and threat of information wars, politicized fakes, that is, attempts to distort historical memory that can trigger processes of delegitimization of the political regime. At the same time, digitalization provides additional prospects for political regimes in terms of the use of social networks by government agencies and the transformation of communication models of parties. Citizens get the opportunity of electronic democracy, participation in monitoring the actions of authorities through special digital platforms and applications. True, on the other hand, accelerated digitalization does not at all exclude the creation of entire Panopticons on the basis of a number of political regimes, within the framework of which flexible technologies for the manipulation of consciousness will be practiced, as well as the establishment of mutual surveillance procedures. Thus, the digitalization process is a kind of civilizational fork, providing both cyber-optimistic and cyber-pessimistic scenarios for political regimes.

This study has delved into the intricate landscape of digital authoritarianism, scrutinizing its multifaceted definitions and implications. The exploration of its manifestations, tools, and strategies employed by authoritarian regimes has provided valuable insights into the ways in which power is wielded, information is controlled, and dissent is stifled in the digital age. Through an analysis of scholarly works, case studies, and real-world instances, this article has underscored the evolving nature of digital authoritarianism, emphasizing its adaptability to technological advancements and its challenge to the fundamental ideals of freedom and democracy.

The study showed that there is no precise definition of digital authoritarianism in the academic literature. Each of the specialists focuses on one of the features of digital authoritarianism. After researching we ended up forming the following definition: Digital authoritarianism, through the help of information technologies, internet censorship, mass surveillance, social media manipulation and data control, is aimed at restricting people's rights to receive information, exchange information, controls and manages people's social behavior, restricts people's social freedoms.

Surveillance, cyberattacks and espionage, censorship, social and electoral manipulation are the main tools that authoritarian regimes use to strengthen their position not only within the country but also beyond its borders. The diverse dimensions of digital authoritarianism were highlighted, ranging from mass surveillance and censorship to cyber attacks and data manipulation. By considering these facets, societies and policymakers can formulate proactive measures to safeguard democratic principles, thwart the encroachment of authoritarian practices, and ensure the unimpeded flow of information. As technology continues to evolve and shape our world, a keen awareness of the nuances surrounding digital authoritarianism will prove essential in preserving the integrity of democratic societies.

The imperative to prevent digital authoritarianism stems from the recognition that its unchecked proliferation could lead to dire consequences. It threatens the essence of open societies by silencing dissent, restricting access to information, and concentrating power in the hands of the ruling elite. The urgency is heightened by its ability to surpass geographical limits, allowing its impact to stretch well past the borders of its originating nations. It is clear that digital authoritarianism is expressed in specific countries, the measures and legal frameworks put in place to counter it, and the impact of fake news on political processes and programs.

The political experience of digitalization of the post-Soviet region demonstrates not only new risks of the democratic trajectory of stability, but also cases of digitalization of authoritarian regime consolidation. In this regard, an urgent scientific task is to measure the digital regime diversification of post-Soviet states not only within the framework of the 'digital authoritarianism - digital democracy' dichotomy, but also on the basis of an analysis capable of recording transitions from one non-democratic regime form to another type of authoritarianism.

Supplementary material

The supplementary material for this article can be found at https://doi.org10.46991/JOPS/2023.2.6.062

Conflict of interests

The author declares no ethical issues or conflicts of interest in this research.

Ethical standards

The author affirms this research did not involve human subjects.

References

Albrecht, Bahia, and Naithani, Gaura. 2022."Digital Authoritarianism: A Global Phenomenon." *Deutsche Welle*. March 17, 2022. Accessed September 29, 2023. https://akademie.dw.com/en/digital-authoritarianism-a-global-phenomenon/a-61136660.

Aleksanyan, Ashot, and Arusyak Aleksanyan. 2022. "Rethinking the Non-Resilience of Trade Unions in Armenia: How to Protect Social Rights and Freedoms of Workers?" *Journal of Political Science: Bulletin of Yerevan University* 1 (1): 78-106. https://doi.org/10.46991/JOPS/2022.1.1.078.

Aleksanyan, Nane. 2022. "Mapping Political Populism in the European Post-Transitional Periphery". *Journal of Political Science: Bulletin of Yerevan University* 1 (2): 73-91. https://doi.org/10.46991/JOPS/2022.1.2.073.

Amnesty International. 2023. "Armenia/Azerbaijan: Pegasus Spyware Targeted Armenian Public Figures amid Conflict." Accessed September 29, 2023. https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/.

BBC. 2021. "Pegasus: Who Are the Alleged Victims of Spyware Targeting?" *July 22, 2021*. Accessed September 29, 2023. https://www.bbc.com/news/world-57891506.

Brandt, Jessica, and Torrey Taussig. 2019. "Europe's Authoritarian Challenge." *The Washington Quarterly* 42 (4): 133-153. https://doi.org/10.1080/0163660X.-2019.1693099.

Ellis, Joseph M. 2022. “Russian Disinformation: The Forest Brothers, Baltic Resistance, and NATO.” In: *Information Wars in the Baltic States: Russia’s Long Shadow*, edited by Janis Chakars and Indra Ekmanis, 35-52. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-99987-2_3.

Factor TV. 2023. “During the war, they tried to spy on the phone of the MFA spokesperson. Samvel Martirosyan: VIDEO.” *May 29, 2023*. Accessed September 29, 2023. https://factor.am/651459.html

Feldstein, Steven. 2019. “The Global Expansion of AI Surveillance.” Washington, DC: Carnegie Endowment for International Peace. Accessed September 29, 2023. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

Freedom House. 2019. “Social Media Are a Growing Conduit for Electoral Manipulation and Mass Surveillance.” Accessed September 29, 2023. https://freedomhouse.org/article/social-media-are-growing-conduit-electoral-manipulation-and-mass-surveillance.

Freedom House. 2022. “Freedom on the Net 2022.” Accessed September 29, 2023. https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.

Glazunova, Sofya. 2022. The “Sovereign Internet” and Social Media. In: Digital Activism in Russia: The Communication Tactics of Political Outsiders. Palgrave Macmillan, Cham, 67-88. https://doi.org/10.1007/978-3-030-93503-0_4.

Gosztonyi, Gergely. 2023. The Rise of Digital Authoritarianism Across the Globe. In: Censorship from Plato to Social Media. Law, Governance and Technology Series, vol 61. Springer, Cham, 157-168. https://doi.org/10.1007/978-3-031-46529-1_11.

Greitens, Sheena Chestnut, 2020. “Dealing with Demand for China’s Global Surveillance Exports.” *The Brookings Institution, April 2020*, Accessed September 29, 2023. https://www.brookings.edu/wpcontent/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf.

Isaacs, Rico. 2022. Non-oligarchic Public Voice in Kazakhstan from Below, 2011-2022. In: Political Opposition in Authoritarianism. The Theories, Concepts and Practices of Democracy. Palgrave Macmillan, Cham, 97-126. https://doi.org/10.1007/978-3-031-06536-1_6.

JAM-news. 2021. “Azerbaijan Suspected of Spying on Journalists Using Israeli Pegasus Spyware.” *July 19, 2021*. Accessed September 29, 2023. https://jam-news.net/azerbaijan-suspected-of-spying-on-journalists-using-israeli-pegasus-spyware/.

Khalil, Lydia. 2020. “Digital Authoritarianism, China and Covid.” *Lowy Institute, November 2, 2020*. Accessed September 29, 2023. https://www.lowyinstitute.org/-publications/digital-authoritarianism-china-covid.

Krapiva, Natalia, and Anastasiya Zhyrmont. 2023. “Digital Dictatorship: Authoritarian Tactics and Resistance in EECA.” *Access Now, March 17, 2023*. Accessed September 29, 2023. https://www.accessnow.org/digital-dictatorship-and-resistance-in-eastern-europe-and-central-asia/.-.

Kravtsov, Vlad. 2022. Securitizing the Epidemic: Ideological Adaptations and Illiberal Meanings. In: Autocracy and Health Governance in Russia. Palgrave Macmillan, Cham, 153-188. https://doi.org/10.1007/978-3-031-05789-2_5.

Michaelsen, Marcus. 2018. “Transforming Threats to Power: The International Politics of Authoritarian Internet Control in Iran.” *International Journal of Communication* 12: 3856-3876.

Mirzoyan, Armen. 2021. “Those who have information about Armenia’s foreign policy are targeted by Pegasus.” *Hetq.am, November 24, 2021*. Accessed September 29, 2023. https://hetq.am/hy/article/138214.

Mölder, Holger. 2019. “The prospects of strategic imagination in explaining international security challenges.” *Quality & Quantity: International Journal of Methodology* 57: 55-76. https://doi.org/10.1007/s11135-022-01386-w.

Mozur, Paul, 2021. “The Great Firewall: China’s model of digital control.” *MIGS Montreal, September 26, 2021*. Accessed September 29, 2023. https://www.youtube.com/watch?v=IMDYzAsomGA.

Perez, Evan, and Diaz, Daniella. “FBI: DNC Rebuffed Request to Examine Computer Servers.” *CNN, January 5, 2017*. Accessed September 29, 2023. https://www.cnn.com/2017/01/05/politics/fbi-russia-hacking-dnc-crowdstrike/index.html.

Polyakova, Alina, and Chris Meserole. 2019. “Exporting digital authoritarianism: The Russian and Chinese models.” *Brookings Institution Policy Brief*. Accessed September 29, 2023. https://www.brookings.edu/wp-content/uploads/2019/-08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Qiaoan, Runya, and Jessica C. Teets. 2020. “Responsive Authoritarianism in China - a Review of Responsiveness in Xi and Hu Administrations.” *Journal of Chinese Political Science* 25: 139-153. https://doi.org/10.1007/s11366-019-09640-z.

Richey, Mason. 2018. “Contemporary Russian revisionism: understanding the Kremlin’s hybrid warfare and the strategic and tactical deployment of disinformation.” Asia Europe Journal 16: 101-113. https://doi.org/10.1007/s10308-017-0482-5.

Roberts, Huw, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. 2021. “The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation.” *AI & Society: Journal of Knowledge, Culture and Communication* 36: 59-77. https://doi.org/10.1007/s00146-020-00992-2.

Rothacher, Albrecht. 2021. Putin’s Autocracy: Siloviki Rule and Their Kleptocracy. In: Putinomics. Springer, Cham, 105-155. https://doi.org/10.1007/978-3-030-74077-1_3.

Schatz, Edward. 2023. “Varieties of Authoritarianism in Eurasia.” In: *Securitization and Democracy in Eurasia: Transformation and Development in the OSCE Region*, edited by Anja Mihr, Paolo Sorbello, and Brigitte Weiffen, 279-290. Springer, Cham. https://doi.org/10.1007/978-3-031-16659-4_19.

Schlumberger, Oliver, Mirjam Edel, Ahmed Maati, and Koray Saglam. 2023. “How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship.” *Government and Opposition*: 1-23. https://doi.org/10.1017/gov.2023.20.

Shahbaz, Adrian. 2018. “The Rise of Digital Authoritarianism: Fake news, data collection, and the challenge to democracy”. Accessed September 29, 2023. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

Sinkkonen, Sinkkonen, and Jussi Lassila. 2022. “Digital Authoritarianism and Technological Cooperation in Sino-Russian Relations: Common Goals and

Diverging Standpoints." In: *Russia-China Relations: Emerging Alliance or Eternal Rivals?*, edited by Sarah Kirchberger, Svenja Sinjen, and Nils Wörmer, 165-184. Springer, Cham. https://doi.org/10.1007/978-3-030-97012-3_9.

Taylor, Monique. 2022. China's Digital Authoritarianism Goes Global: A Governance Perspective. In: China's Digital Authoritarianism. Politics and Development of Contemporary China. Palgrave Macmillan, Cham, 111-130. https://doi.org/-10.1007/978-3-031-11252-2_6.

Williams, Martyn. 2010. "North Korea Moves Quietly onto the Internet." *Computerworld, June 10, 2010.* Accessed September 29, 2023. https://www.computerworld.com/article/2518914/north-korea-moves-quietly-onto-the-internet.html.

Woodhams, Samuel, 2020. "The Rise of Internet Throttling: A Hidden Threat to Media Development." *Center for International Media Assistance, May 20, 2020*. Accessed September 29, 2023. https://www.cima.ned.org/publication/the-rise-of-bandwidththrottling-a-hidden-threat-to-media-development/.

Yang, Yuan, and Madhumita Murgia, 2019. "Data leak reveals China is tracking almost 2.6m people in Xinjiang." *Financial Times, February 16, 2019*. Accessed September 29, 2023. https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812.

Yaybokeand, Erol, and Samuel Brannen. 2020. "Promote and Build: A Strategic Approach to Digital Authoritarianism." *Center for Strategic and International Studies (CSIS), October 15, 2020.* Accessed September 29, 2023. https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.

Yilmaz, Ihsan, and Fan Yang. 2023. "Digital Authoritarianism, Religion and Future of Democracy." In: *Digital Authoritarianism and its Religious Legitimization: The Cases of Turkey, Indonesia, Malaysia, Pakistan, and India*, edited by Ihsan Yilmaz, 151-166. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-99-3600-7_7.

Yilmaz, Ihsan. 2023. "Digital Authoritarianism and Religion in Democratic Polities of the Global South." In: *Digital Authoritarianism and its Religious Legitimization: The Cases of Turkey, Indonesia, Malaysia, Pakistan, and India*, edited by Ihsan Yilmaz, 1-19. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-99-3600-7_1.

Zheng, Wang. 2020. "What Is WeChat and What Can It Do?" *CGTN, August 9, 2020*. Accessed September 29, 2023. https://newseu.cgtn.com/news/2020-08-09/What-is-WeChat-and-what-can-it-do--SNepY1rgNG/index.html.