Domestic Decision-Making, Regional Linkages, and Cybersecurity Considerations: Implementation of Internet Voting in Russia, September 2021

Logan Carmichael[1,2] and Bogdan Romanov[1,3][0000-0001-8594-2387]

[1] Johan Skytte Institute of Political Studies, University of Tartu, Tartu, Estonia
[2] logan.emily.carmichael@ut.ee
[3] bogdan.romanov@ut.ee

Abstract. The research objective of the article is to explain why and how the Russian Federation implemented online voting in the case of the September 2021 national State Council elections. This case constitutes the first instance of large-scale, non-democratic, and legally binding elections with the use of i-voting. Hence, the paper provides answers to (1) why i-voting was introduced in the already state-controlled electoral context, (2) how Estonia, as a cradle of i-voting, affected the decision-making in Russia, and (3) how cybersecurity concerns were addressed by technology providers and engage in a discussion about cybersecurity not for users, but for officials. Our research design focuses on the instance of Russian online voting without going into further details of regional and capital city distinction and relies on the interview data. Results show that (1) the primary motivation underpinning the introduction of i-voting in Russia was regime stability, (2) Estonian successes in e-governance and i-voting did not impact decision-making in Russia, and (3) cybersecurity concerns around the i-voting technologies used in Russia were indeed present but were not central to decision-making. Findings have broader implications, the research fills in a gap in the literature surrounding the emergence of i-voting, as well as the relationship these processes have with existing, longer-term implementations in democratic states. At the same time, from the empirical viewpoint, the work sheds light on how topics in non-democracies can be studied.

Keywords: i-voting· cybersecurity· Russia · digital authoritarianism

1 Introduction

Electronic governance (e-governance), initially an undertaking in predominantly democratic states, has more recently become popular in some non-democratic regimes as well. This trend could be observed around 2015 [1; 2] when Internet penetration was no longer a uniquely democratic feature. As a result, this non-democratic shift led to the implementation of online participatory practices in autocratic states (e.g., China [3; 4], Egypt [5], post-soviet states, Kazakhstan [6], Kyrgyzstan [7], and others).

Even though the academic community noticed non-democratic interest in digital political technologies, some topics are overlooked, for instance, the recent online elections in Russia in September 2021. This is a continuation of previous trials in Moscow in 2019, however, this time opportunity to vote online was available in seven regions of Russia. Although limited in scale, this new i-voting precedent caused considerable discussions on the Internet, especially as tallying of online votes was exposed to be fraudulent [8]. Yet, the discussion did not draw any lessons or further implications for the i-voting implementation in Russia. This is an essential remark since March 14, 2022, online voting can be used in all elections in Russia.

Thus, the article's main research objective is to shed light on the rationale behind the introduction of i-voting in Russia, even though the party in power already controlled the electoral field. Secondly, this article explores how digital governance, i-voting, and cybersecurity success in neighboring Estonia impacted decision-making in Russia. Finally, this article aims to explain how aspects of cybersecurity were addressed.

2 Theoretical background and hypotheses

This paper employs twofold digital authoritarianism and a constructivist approach to the topics of i-voting and cybersecurity in Russia. Together, these two theoretical groundings provide a useful explanatory lens through which to examine these topics.

In its adoption of a digital authoritarianism approach, this paper employs various literature strands that refer to the use of the Internet and e-governance technologies in non-democratic contexts [9; 10]. The main contribution of the theoretical approach is that "…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." [11, p. 2] With this backbone in mind, we will unpack the rationale behind implementing online voting in Russia. Additionally, the focus on political and social control would imply flawless cybersecurity of the deployed technology.

Specifically, the constructivist approach enacted here would borrow from constructivist theory in international relations, emphasizing the centrality of ideation and experiences in behavior, interactions, and political decision-making [12]. Although this paper looks at i-voting as an inherently domestic undertaking in Russia, it is an endeavor with international ramifications, as traditional understandings of jurisdiction become quickly blurred in cyberspace and the digital world. Ciolan [13] has written specifically about how a constructivist approach is useful to the study of cybersecurity because involved stakeholders are "trying to impose their ideas regarding the way of constructing the future type of cyberspace" [13, p. 131]. This broad premise extends to i-voting and governance decisions surrounding the implementation of i-voting.

Leaving literature review aside, we derived the following hypotheses from the current state-of-the-art:

H1: Online voting was implemented solely as a tool for regime stability via electoral fraud and results manipulation

This assumption stems directly from the digital authoritarianism theory, which entails that all digital and technological alterations are caused because of regime instability. However, the case of the September 2021 elections could have more than one explanation. COVID-19 could be another reason behind the i-voting introduction since autocracies care about their population as a source of legitimacy. That is why autocracies might be more reactive due to the 'autocratic advantage' [14] in protecting their citizens [15; 16]. Or it could be a consequent step in developing the e-governance ecosystem in Russia, which could be traced from Medvedev's presidential term in 2008-2012.

H2: Regional competition between Estonia and Russia did play a crucial role in the establishment of online voting

Taking into account all the perturbations in Russia-Estonia relationships, we assume that Estonia could, in a form of collaboration or competition, incentivize further development of e-governance in Russia. Either Russian officials could refer for help to the Estonian side, or maybe there were discourses which hinted that Russia was driven by a desire to prove to be on par with a digitally advanced neighbor. This assumption is supported by the digital authoritarianism paradigm, which emphasizes regime maintenance, and here, this collaboration/competition would give Russia more international legitimacy as a capable state.

H3: Cybersecurity concerns were at the core of decision-making regarding the online voting implementation

Since it is not the first online voting trial in Russia, but the first on such a large scale, we would expect decision-makers and providers of the technology to think through the cybersecurity aspect of the elections. Especially after the cases in which elections were hijacked from the outside of a state, conducting elections. Additionally, as described in the literature, Russia has a unique approach toward cyberspace and, thus cybersecurity, so this question should be among the first priorities.

As a result, these three hypotheses will expose genuine rationales behind the implementation of online voting in the case of the 2021 elections; analyze the role of Estonia in the decision-making process; and finally, will shed more light on the perception of cybersecurity in Russia, which is expected to be different from the democratic one.

3 Methodology

The research employs a qualitative empirical design, which consists of semi-structured interviews. The semi-structured expert interviews will help us to gather domain knowledge from people inside of Russia, people specializing in Russia, and experts outside of Russia. By employing semi-structured interviews, we could gain nuanced insight into these ideas and experiences surrounding i-voting and cybersecurity issues. As a result, we will have corpora of texts, which could prove or falsify our hypotheses. Since hypotheses cover different topics, we applied purposive sampling [17] to cover every assumption. As a result, we pinpointed three groups of respondents with a different number of people in each, see Table 1.

Table 1. The list of interviewees from different areas of expertise.

Group name	Quantity	Affiliation
Political scientists	**4**	Universities in Russia, Finland
I-Voting practitioners/ decision-makers	**4**	State Information System, National election committee, University of Tartu
Cybersecurity practitioners	**2**	Cybernetica, e-Governance Academy

As a remark, we would like to address the question of our respondents' anonymity since we are working with a susceptible topic. First, respondents were asked to sign an informed consent form, in which they could choose to stay anonymous or allow us to mention their names. Secondly, despite the answer in the form, we anonymized all interview audio recordings and stored them in a secured and different folder from the one with consent forms. Lastly, we sent transcripts to the respondents for their approval.

4 Results

This paper has shed light on Russian internet voting processes, the decision-making behind its implementation, how it has been impacted by regional players and trends, and the cybersecurity of i-voting technologies in the September 2021 elections.

Firstly, it has examined the role of regime stability in the decision to implement i-voting in Russia, finding that indeed considerations such as the possibility to manipulate electoral outcomes digitally, cost efficiency for the incumbent, and the lack of in-person voting interactions aimed to prevent political violence or protests all offer compelling motivations for the Russian authorities.

Secondly, it has been found that Estonia's early and pervasive adoption of e-governance practices and, specifically, i-voting did not impact Russian decision-making around the implementation of i-voting on the grounds of regional competition; rather, Russia may have seen Estonia as a benchmark in this space but crafted its system, with distinct i-voting technologies. Rather than regional competition between Russia and Estonia, this paper suggests regional cooperation on digital governance between Russia and other non-democratic regimes in the region.

Finally, this paper examined cybersecurity concerns with Russian i-voting technologies, discovering linkages between cybersecurity and the previously outlined regime stability. The degree to which Russian authorities feared interference with their elections is not necessarily represented in the cybersecurity mechanisms protecting i-voting technologies. Concerns with authentication and with source code that lacks transparency were not addressed and left the possibility of electoral manipulation, indicating that cybersecurity concerns were not at the forefront of decision-making for Russian authorities; rather, there is the possibility that they were intentionally neglected, in some capacities, for the purpose of regime stability. In outlining these interconnected topics of i-voting, regime stability, and cybersecurity, this paper has also illuminated interesting trends in i-voting practices and diffusions in a non-democratic context, providing novel directions for future research on these topics.

References

1. Kabanov, Y., Romanov, B.: Interaction Between the Internet and the Political Regime: An Empirical Study (1995–2015). Digital Transformation and Global Society. pp. 282–291. Springer International Publishing, Cham (2017).
2. Karlsson, M.: Carrots and sticks: internet governance in non-democratic regimes. IJEG. 6, 179 (2013). https://doi.org/10.1504/IJEG.2013.058405.
3. Deng, J., Liu, P.: Consultative Authoritarianism: The Drafting of China's Internet Security Law and E-Commerce Law. Journal of Contemporary China. 26, 679–695 (2017). https://doi.org/10.1080/10670564.2017.1305488.
4. Kornreich, Y.: Authoritarian responsiveness: Online consultation with "issue publics" in China. Governance. 32, 547–564 (2019). https://doi.org/10.1111/gove.12393.
5. ELKheshin, S., Saleeb, N.: Assessing the Adoption of E-government Using Tam Model: Case of Egypt. IJMIT. 12, 1–14 (2020). https://doi.org/10.5121/ijmit.2020.12101.
6. Amanbek, Y., Balgayev, I., Batyrkhanov, K., Tan, M.: Adoption of e-Government in the Republic of Kazakhstan. JOItmC. 6, 46 (2020). https://doi.org/10.3390/joitmc6030046.
7. Sheranova, A.: Cheating the Machine: E-voting Practices in Kyrgyzstan's Local Elections. European Review. 28, 793–809 (2020). https://doi.org/10.1017/S1062798720000241.
8. Jiménez, R., Thurner, S., Pericchi, L.R., Klimek, P.: Fraud Detection, Electoral. In: Balakrishnan, N., Colton, T., Everitt, B., Piegorsch, W., Ruggeri, F., and Teugels, J.L. (eds.) Wiley StatsRef: Statistics Reference Online. pp. 1–10. Wiley (2018). https://doi.org/10.1002/9781118445112.stat08006.
9. Cebul, M., Pinckney, J.: Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution. 24 (2021).
10. Dragu, T., Lupu, Y.: Digital Authoritarianism and the Future of Human Rights. Int Org. 75, 991–1017 (2021). https://doi.org/10.1017/S0020818320000624.
11. Yayboke, E., Brannen, S.: A Strategic Approach to Digital Authoritarianism. 12 (2020).
12. Theys, S.: Introducing Constructivism in International Relations Theory. International Relations. 4 (2018).
13. Ciolan, I.M.: Defining Cybersecurity as the Security Issue of the Twenty First Century. A Constructivist Approach. 17 (2014).
14. Schwartz, J.: Compensating for the 'Authoritarian Advantage' in Crisis Response: A Comparative Case Study of SARS Pandemic Responses in China and Taiwan. J OF CHIN POLIT SCI. 17, 313–331 (2012). https://doi.org/10.1007/s11366-012-9204-4.
15. Cepaluni, G., Dorsch, M.T., Branyiczki, R.: Political Regimes and Deaths in the Early Stages of the COVID-19 Pandemic. 49 (2020).
16. Cheibub, J.A., Hong, J.Y.J., Przeworski, A.: Rights and Deaths: Government Reactions to the Pandemic. SocArXiv (2020). https://doi.org/10.31235/osf.io/fte84.
17. Turner, D.: Qualitative Interview Design: A Practical Guide for Novice Investigators. TQR. (2014). https://doi.org/10.46743/2160-3715/2010.1178.