Digital Authoritarianism and NATO's Security Agenda: Implications for the Eastern Flank

Author: Aleksandre Buzaladze

Contents

Introduction

Digital authoritarianism has become one of the most significant security challenges that confronts democratic states and international organizations in the 21st century. The rapid expansion of digital technologies has allowed authoritarian regimes to refine methods of repression, censorship, surveillance and psychological manipulation. These regimes increasingly use digital tools not to control populations at home but also to influence or destabilize societies abroad. Scholars refer to this trend as digital authoritarianism, which in Russian context is called networked authoritarianism (Michaelsen & Ruijgrok, 2024; Lokot, 2023).

For the North Atlantic Treaty Organization, digital authoritarianism poses a direct challenge to its strategic goals and collective defense responsibilities. Russia's broad use of information manipulation, cyber operations and the control of digital infrastructure has grown significantly since 2014, intensifying after the full-scale invasion of Ukraine in 2022. These practices directly target Eastern Flank of NATO, where states such as Poland, the Baltic republics, Romania and others remain vulnerable to disinformation campaigns and hybrid actions designed to weaken democratic institutions and reduce confidence in the alliance.

NATO has acknowledged the seriousness of this threat. A 2021 NATO Review report highlighted disinformation and digital interference as core challenges to the alliance's resilience. It warns that adversaries exploit the openness of democratic societies to spread false information, inflame social divisions and erode trust in public institutions (NATO Review, 2021). At the same time, NATO's strategic documents emphasize the need to increase collective defense spending to five percent of GDP by 2035, while integrating new digital resilience measures that address the complexities of modern information environments.

Paper argues that digital authoritarianism represents a strategic threat to NATO's Eastern Flank because it simultaneously targets public trust, political cohesion, military readiness and integrity of democratic institutions. By examining the theoretical foundations of digital authoritarianism, analyzing Russian practices in Ukraine and surrounding regions, evaluating NATO's existing countermeasures and proposing practical recommendations, this paper aims to contribute to a strategic understanding of how the alliance can adapt to the evolving digital landscape.

Conceptual Framework

Digital authoritarianism refers to the systematic use of digital technologies by authoritarian governments to monitor, control or manipulate domestic and international information environments (Michaelsen & Ruijgrok, 2024). Unlike classical authoritarianism, which relies heavily on physical coercion, digital authoritarianism employs advanced technological tools that allow more targeted and efficient forms of control. Scholars identify several core components of digital authoritarian governance.

- **Digital surveillance.** This includes the monitoring of communications, social media and movement through the use of data collection systems, artificially intelligent monitoring and biometric technologies.
- **Information control.** Authoritarian regimes control or restrict access to independent media, filter online information and censor platforms that challenge the narrative of the state.
- **Network manipulation.** These techniques include coordinated disinformation campaigns, the use of trolls and bots, algorithmic amplification of political messages and the strategic spread of false or misleading information.
- **Infrastructure control.** States may impose internet shutdowns, re-route digital traffic or establish centralized digital systems that eliminate external oversight.

These practices allow authoritarian states to exploit the vulnerabilities of open societies. According to Marechal (2017), authoritarian digital influence extends well beyond domestic borders. Technologies and governance models developed within authoritarian systems increasingly travel across borders, strengthening a global ecosystem of illiberal digital practices. The transnational nature of these tools makes digital authoritarianism a strategic challenge on multiple levels, ranging from national security to societal trust.

In the framework of NATO's Eastern Flank the most relevant actor is Russia, which combines domestic digital repression with sophisticated external operations. This hybrid approach, described by Lokot (2023) as networked authoritarianism, integrates digital censorship, surveillance and information manipulation within a broader geopolitical strategy. Russia uses digital tools to influence public opinion, control populations in occupied territories and disrupt the political cohesion of NATO member-states.

Thus, digital authoritarianism is both a domestic governance structure and a foreign policy instrument. Its importance for NATO lies in its ability to undermine democratic processes, polarize societies and weaken collective defense mechanisms without engaging in traditional military conflict.

Russia's Networked Authoritarianism and Its Projection Abroad

Russia represents the clearest example of a state that uses digital technologies as part of a broader strategy to influence, pressure and destabilize neighboring democracies. Its model of networked authoritarianism combines domestic information control with an extensive capacity for external disinformation, digital manipulation, surveillance and cyber operations (Lokot, 2023; Marechal, 2017). For NATO's Eastern Flanks this projection of digital authoritarian techniques has been particularly impactful in the Baltic States, Poland and the broader Black Sea region.

In the **Baltic States,** Russian influence is particularly pronounced. Estonia, Latvia and Lithuania have long been the target of hostile narrative strategies designed to erode trust in democratic institutions and to question the legitimacy of NATO's presence. The International Centre for Defence and Security (ICDS) report on Baltic resilience underscores that these states draw on historical memory of totalitarianism and occupation, as well as a regional context of cross-sectoral cooperation, to build disinformation resistance (Teperik et al., 2022). Nevertheless, they remain exposed: disinformation campaigns exploit linguistic divides, promote conspiratorial narratives and mobilize cross-border influence networks, demonstrating how Russia's digital authoritarianism weaponizes local grievances (Teperik et al., 2022).

Poland is similarly exposed to Russian digital influence. Moscow's operations in Poland exploit political cleavages, historical tensions and skepticism toward NATO, aiming to destabilize pro-Western narratives. These campaigns often rely on online content networks, troll amplification and disinformation dresses as domestic commentary. Such tactics align with the hybrid threat model described by the NATO Strategic Communications Centre of Excellence, where hostile state actors combine information manipulation, cyber tactics and ambiguity to undermine public trust (Gill & Hansen, 2021). Moreover, cyber intrusions into Polish governmental and institutional systems have aimed to erode administrative capacity and elevate uncertainty in the public sphere, fitting into a broader strategic campaign to weaken Baltic-Policy cohesion within NATO.

In the **Black Sea region,** where NATO's strategic and energy interests are especially acute, Russia's digital authoritarianism plays a crucial geopolitical role. In states like Romania and Bulgaria, disinformation narratives question NATO's naval operations, cast doubt on reform processes and play on historical mistrust of Western institutions. These narratives are disseminated via Russian-aligned media outlets, social platforms and covert influence networks. At the same time, cyber operations targeting infrastructure, such as energy networks or government systems, create operational risk, undermine public confidence and increase the political cost of Western alignment. Strategic communications research from the StratCom COE warns that these hybrid measures, combining cyber, legal and information instruments are precisely the kind of "grey-zone" hostile measures adversaries use to exert influence without open conflict (Gill & Hansen, 2021).

Through these mechanisms, Russia's networked authoritarianism does more than influence public opinion: it seeks to degrade institutional resilience, sow societal divisions and ultimately weaken NATO's foothold in regions that are pivotal for collective defense.

Strategic Implications for the Eastern Flank

The Eastern Flank of NATO, comprising the Baltic countries, Poland, and the black Sea region, faces heightened vulnerability to Russia's networked authoritarian tactics. These threats carry profound strategic implications not only for national resilience, but also for alliance cohesion and collective defense.

Undermining public trust and democratic cohesion

Russian disinformation and influence operations in the Baltic States and Poland seek to erode trust in democratic institutions and question the legitimacy of NATO. By exploiting historical grievances, language divides and social cleavages such campaigns aim to weaken societal cohesion. The ICDS report underscores that Latvia, for instance, faces greater difficulty in resisting disinformation than its Baltic neighbors because of demographic and linguistic vulnerabilities (Teperik et al., 2022). These dynamics threaten to fracture domestic unity and reduce public support for defense cooperation.

Strategic divergence within NATO

If public trust in NATO weakens, so does political willingness to commit to common defense. Disinformation that frames NATO presence as intrusive or hostile can influence political debates, elections and defense postures. Over time, this may degrade the political will of Eastern Flank states to maintain unified support for collective defense, potentially encouraging strategic divergence.

Operational risks and resilience challenges

Cyber intrusions and influence campaigns in Eastern Flank countries undermine not just domestic governance but also NATO operational readiness. Persistent digital pressure can distract governments, degrade institutional capacity and compromise decision-making during crises. For example, Russian cyber tactics targeting infrastructure in Bulgaria or Romania could disrupt critical systems in wartime scenarios, impairing NATO's ability to respond rapidly (Gill & Hansen, 2021).

Long-term erosion of deterrence

Perhaps most troubling is the erosion of long-term deterrence. If digital authoritarianism succeeds in undermining democratic resilience, NATO's strategic advantage is weakened. The Alliance's credibility depends on the strength of its collective institutions and the trust its citizens place in them. Should Russia destabilize these institutions or create fissures in public sentiment, the credibility of NATO deterrence may erode.

Challenge to values-based legitimacy

Finally, these operations challenge NATO's foundational values. Resisting digital authoritarianism is not merely a technical contest, it is a value-based struggle. As hybrid threats increasingly exploit disinformation, cognitive manipulations and AI-enabled influence, NATO must protect not only its military capabilities, but also the open, democratic societies that underpin its legitimacy. The ethical complexity of using AI defensively, as discussed by Van Diggelen et al. (2025), highlights that need for a values-consistent approach.

NATO's Current Approach and Strategic Gaps

NATO has recognized hybrid threats, including disinformation and cognitive warfare, as fundamental challenges. The Alliance's strategic communications efforts, institutional capacity building and resilience initiatives reflect awareness. But despite these efforts, substantial gaps remain in NATO's posture, especially when confronting the evolving digital authoritarian tactics deployed by Russia.

First, NATO's reliance on **strategic communications frameworks** remains primarily reactive. The *Strategic Communications Hybrid Threats Toolkit* produced by NATO's StratCom Centre of Excellence provides a structured model to identify adversary narratives, map hostile actors and prioritize vulnerable audiences (Gill & Hansen, 2021). The toolkit emphasized the need for a "whole-of-state" and "whole-of-society" mindset, pointing to hybrid threats that combine disinformation, cyber operations, economic coercion and plausible deniability. Yet, in practice, NATO's countermeasures often focus on post facto attribution and mitigation rather than preventive narrative disruption or pre-emptive resilience strengthening.

Second, **coordination across member states** remains uneven. While some NATO members on the Eastern Flank have invested significantly in national disinformation resilience, others lack capacity or institutional frameworks to respond effectively. The ICDS report highlights that Baltic states, though relatively advanced in resilience, still rely on fragmented multilevel efforts involving civil society, media, academia and government (Teperik et al., 2022). NATO's challenge is to align these disparate national efforts into a coherent alliance-wide strategy.

Third, **technological and analytical capacities to counter advanced cognitive warfare** are underdeveloped. Emerging threats, including AI-driven influence operations and algorithmic amplification, pose dual-use risks. The *Wired for War* report by MIGS demonstrates that authoritarian regimes are weaponizing artificial intelligence, deep fakes, bots and algorithmic content to scale foreign information manipulation operations (Matthews & Lamensch, 2025). NATO's existing early-warning and resilience measures are not yet fully equipped to detect and counter these AI-enabled operations at scale.

Fourth, **ethical and legal constrains** complicate the deployment of active countermeasures. While using AI to defend against cognitive warfare shows promise, scholars caution that it raises significant rights-related risks. Van Diggelen, Aidman, Rowa and Vince (2025) propose AI-enabled systems that can counter malicious digital influence, but they emphasize the need for human oversight, transparency and respect for civil liberties (Van Diggelen et al., 2025). Unregulated use of surveillance, content moderation or automated takedowns risks undermining democratic norms, the values NATO is designed to protect.

Finally, **resilience remains insufficiently institutionalized.** NATO's Strategic Foresight Analysis (ACT) outlines long-term scenarios involving hybrid and cognitive domains yet translating scenario planning into structural capacity is lagging (Allied Command Transformation, 2023). Moreover, building resilience required deeper engagement with civil society, media and private sector actors – actors that NATO has not fully integrated into its core strategic planning.

NATO has the conceptual tools to confront hybrid and digital authoritarian threats, but needs to close the gap between strategy and implementation. Without stronger analytical, technological and institutional investments, the Alliance may struggle to respond effectively to increasingly sophisticated influence operations.

Policy Recommendations

To address the challenges posed by digital authoritarianism, NATO should implement a comprehensive set of policy measures that strengthen resilience, improve coordination and modernize defensive capabilities.

- **Strengthen alliance wide digital resilience**

NATO should establish a standardized framework for digital resilience that includes national digital readiness assessments, shared threat intelligence and common operational protocols. This would help reduce disparities across member states.

- **Enhance cooperation with the EU**

Digital authoritarianism threats cross institutional boundaries. NATO should expand cooperation with the EU in areas such as cybersecurity, information integrity and infrastructure protection.

- **Expand AI assisted detection**

The alliance should invest in artificially intelligent systems capable of monitoring emerging disinformation campaigns, tracking coordinated online activity and identifying algorithmic manipulation. These tools should operate within democratic and privacy protecting frameworks.

- **Increase support for frontline member states**

The Eastern Flank requires targeted support due to higher exposure to digital authoritarian tactics. NATO should provide financial assistance, training programs and technical expertise to strengthen resilience in these states.

- **Integrate civil society and the private sector**

NATO should build partnerships with technology companies, academic institutions and civil society organizations. These actors possess critical expertise in areas such as media literacy, fact checking and data security.

- **Develop an alliance wide doctrine for digital conflict**

NATO needs a unified doctrine that clearly defines threats, outlines response mechanisms and establishes norms for engagement. This doctrine should emphasize democratic values and transparency.

- **Strengthen counter disinformation campaigns**

NATO communication strategy should promote authoritative information, enhance transparency and counteract false narratives. Public awareness campaigns can reduce vulnerability to manipulation.

Conclusion

Digital Authoritarianism represents one of the most vital contemporary challenges to NATO's security landscape, particularly along its Eastern Flank where the Alliance faces the most sustained exposure to Russian influence operations, hybrid tactics and digital coercion. The combination of disinformation, cyber intrusions, algorithmic manipulation and strategic communications warfare demonstrates that authoritarian states increasingly employ digital tools not only to shape their domestic environments but also to influence democratic states in ways that erode governance capacity, societal trust and political cohesion. As the earlier sections of this paper showed, Russia projects networked authoritarianism into the Baltic States, Poland and the Black Sea region through coordinated information campaigns, targeted cyberattacks and psychological operations that exploit social cleavages, historical traumas and institutional vulnerabilities.

NATO has taken steps to confront these challenges, but substantive gaps remain between strategic intent and operational capacity. While the Alliance has developed analytical tools, strategic communications frameworks and long-term foresight assessments, its posture remains uneven across member states and insufficiently aligned with the speed and sophistication of Russian digital authoritarian tactics. Moreover, emerging artificially intelligent manipulation capabilities and cognitive warfare strategies further complicate NATO's ability to respond without compromising democratic values. These complexities underscore the need for NATO to adopt more comprehensive and proactive measures, deepen cooperation with civil society and private technology sectors and invest in analytical, technological and institutional capacities that match the scale of the threat.

The strategic implications for NATO's Eastern Flank are critical. Persistent digital interference risks undermining public trust in democratic institutions, weakening political support for allied cooperation and eroding the deterrent posture that underpins collective defense. For the Alliance to preserve both its strategic credibility and its normative foundation, it must integrate digital resilience into its core defense planning and treat information integrity as essential to territorial integrity. The long-term stability of the Baltic States, Poland and the Black Sea region will depend on NATO's ability not only to counter digital authoritarianism, but also to strengthen the societal resilience and democratic confidence that these operations seek to undermine. In this sense, the challenge posed by digital authoritarianism is not simply technological but profoundly political. Hence, meeting it effectively will require coordinated, values based and forward-looking action across the entire Alliance.

References

Allied Command Transformation. (2023). *Strategic foresight analysis 2023*. NATO ACT.

Codreanu, C. M. (2022). *Using and exporting digital authoritarianism: Challenging Both Cyberspace and Democracy.* National University of Political Studies and Public Administration. Europolity, 16(1).

Durojaye, H., & Raji, O. (2022). Impact of state and state sponsored actors on the cyber environment and critical infrastructure. arXiv.

Gill, P., & Hansen, L. (2021). *Strategic communications hybrid threats toolkit*. NATO Strategic Communications Centre of Excellence.

Kalathil, S. (2017). *The evolution of authoritarian digital influence.* PRISM, 7(3).

Lokot, T. (2023). *Russia's networked authoritarianism: Control and resilience.* LSE Public Policy Review.

Maréchal, N. (2017). *Networked authoritarianism and the geopolitics of information.* Media and Communication, 5(1).

Matthews, K., & Lamensch, M. (2025). *Wired for war: How authoritarian states weaponize artificial intelligence against the West*. Montreal Institute for Genocide and Human Rights Studies.

Michaelsen, M., & Ruijgrok, K. (2024). *Digital authoritarianism*. In The Oxford handbook of authoritarian politics. Oxford University Press.

NATO Review. (2021). *Countering disinformation: Improving the Alliance's digital resilience.* NATO Review.

Teperik, D., Sahebzadeh, S., Dalla, R., & Kaljula, V. (2022). *Resilience against disinformation: The Baltic experience*. International Centre for Defence and Security.

Van Diggelen, F., Aidman, E., Rowa, H., & Vince, J. (2025). *Countering cognitive warfare with artificially intelligent systems: Threats, opportunities, and rights related risks.* arXiv.

Zannettou, S., Caulfield, T., Setzer, W., Sirivianos, M., & Blackburn, J. (2019). *Disinformation warfare: Understanding state sponsored trolls on Twitter*. *arXiv*. https://arxiv.org/pdf/1901.05997