Russian Digital PSYOPS in CEE

29 NOVEMBER 2025
Delfina Ertanowska



Delfina Ertanowska[1]

RUSSIAN DIGITAL DIPLOMACY – PSYOPS CAMPAIGNS IN CENTRAL EASTERN EU

Russia uses various tools, from cyberattacks, cyber criminality, stealing data, to legal ones such as online campaigns, fake news, hate speech, trolling, or using graphic forms such as cartoons and memes to ridicule and discredit the opponent. This part of the hybrid warfare (which is a part of Russian digital diplomacy – mostly shared propaganda and manipulated content) is carried out using all internet channels, social media and platforms. I**n**

cyber develop era, PSYOPS automatically use the digital domain like cyber activism, hacktivism, preparation for non violent resistance, but not only in traditional way which is described in Ivan Marovic's in his step-by-step guide called "The Path of Most Resistance" (Marovic, 2018). Of course it uses tactics, but tools have changed during the last 20 years. Starting from sponsored articles, favourable and often paid media in the EU, manipulated videos (such as those presenting Ukrainian soldiers in an unfavourable light) to fake comments on social media, manipulated and altered photographs, mocking cartoons or memes which, as a popular means of entertainment and communication in society, create in their own way a view of reality among users. Manipulated content in the form of videos and articles most often appears on Telegram, Viber and X platform channels, which allows them to efficiently bypass EU sanctions, thus allowing users to easily access such content without the need to install a VPN. Memes and cartoons are already appearing in all social media, and while they can be treated as free artistic creation, they are also an element of well-paid campaigns. In Poland, for example, there are companies that provide services of creating marketing and political campaigns through memes (Ertanowska, 2021, p.187-195). Russia is a step further, using subliminal action to give the impression that the majority of society thinks in one way or another.

These include anti-Ukrainian campaigns conducted with particular intensity in Poland and Slovakia, anti-immigration campaigns conducted throughout Europe (like Poland) (Walker, 2025), alleged promotion of "traditional values" aimed at slandering life in Western Europe and negating progress. Pro-Russian campaigns in Latvia and Estonia. Are targeted hybrid attacks aimed not only at inciting antagonisms and social polarisation but also at having a real impact on the election of politicians or on cybersecurity and military security, as in the recent cases in Poland and Romania.

How psychological-information campaigns, both in the framework of Russian hybrid warfare and digital diplomacy, influence the polarisation of society and have a real impact on politics and the security of NATO's eastern flank? This paper aims to highlight and expose the use of psychological-information campaigns applied within digital diplomacy in the context of the use of digital, visual communication and social media to spread disinformation, hate speech, and trolling. The paper focuses primarily on social media and the use of digital communication as a propaganda tool for conducting both soft power disinformation through digital diplomacy, but also as a tool of hybrid warfare in PSYOP campaigns aimed at destabilising social order, politics, and security on NATO's eastern flank.

It can be this photo as a visualisation. https://www.shutterstock.com/pl/image-illustration/fake-news-propaganda-conspiracy-theories-disinformation-2250456551

Hybrid & Information Warfare: Media propaganda, spreading antagonisms via social media using tools such as manipulated photos, videos,

memes, deepfakes, fake news, often created by AI tools. These operations include "active measures" reminiscent of Cold War tactics, aiming to undermine Western democracies, influence elections (e.g., Brexit, EU-Ukraine agreements), and discredit the EU and NATO.

· Troll Farms and Propaganda Networks: The GLOBSEC Policy Institute documents coordinated disinformation across Slovakia, Hungary, and the Czech Republic, last time in Poland, urging cooperation across intelligence, media, and education sectors to counter these threats. Also, media reports and V4 groups reported it.

· Localized Disinformation: In example Estonia, Russian operations include financial, political, and cyber components aimed at manipulating internal affairs. A notable example is the 2007 cyberattack, widely viewed as a strategic disinformation operation. In Poland: cyberattacks, arson, disinformation, racial and religious hate campaigns.

· Pro-Kremlin Messaging Networks: The Doppelgänger campaign (Alaphilippe & Machado & Miguel & Poldi, 2022) digital diplomacy PSYOPS campaigns. The Pravda network pushes millions of pro-Russian articles annually. Its content infiltrates platforms like Wikipedia, AI models, and social media, seeking to influence public opinion and AI-generated outputs worldwide.

· Social Media: like Telegram, Viber, X, as platforms to build "underground Guerrilla" often called the 5th column, in Central Eastern members of the EU.

In 2024, the presidential elections were annulled by the Romanian Constitutional Court due to serious irregularities, including external interference, which undermined their fairness and transparency. The main allegations concerned the illegal use of digital technologies (buying followers, bots, fake content and accounts), artificial intelligence, and covert financing of the election campaign. Both national and international institutions confirmed (Pelin, 2025) that these activities were aimed at supporting the pro-Russian candidate, Călin Georgescu. This is one of the most striking examples of the use of digital diplomacy and psychological operations (PSYOPS) by Russia in the Central and Eastern European region.

According to the report of the Romanian Prosecutor General, Russian entities were involved in disinformation campaigns during the 2024 presidential elections. Advanced digital technologies were used, including bots, trolling, and AI, to generate and disseminate content aimed at fuelling social tensions, polarisation, and hate speech – which also translated into real criminal incidents. One of the tactics of this psychological-information operation was the use of hashtags – in this case, the word "revolution" – in order to mobilise and manipulate public opinion. Additionally, four companies with clear links to the Russian Federation were identified as responsible for disinformation activities directly targeting Romanian society (Dumitrescu, 2025).

Another tactic used in this cyber operation was the fairly common method of using social media platforms – in particular TikTok, Telegram, and X (formerly Twitter) – to spread false information. One of the leading fake news items was a manipulated video falsely claiming that French troops stationed in Romania were disguised in Romanian gendarmerie uniforms in order to interfere in the elections (Blackburn, 2025). Romania's Ministries of Foreign Affairs, Internal Affairs, and Defence issued a joint statement condemning these disinformation activities as Russian interference in the electoral process.The decision of the Constitutional Court to annul the elections provoked controversy both domestically and abroad, and the issue of the Romanian elections made headlines around the world. Călin Georgescu himself, who had obtained the highest result in the first round of the elections, condemned the decision as a coup d'état. His rival, Elena Lasconi, in turn, warned of the threat to democracy. International observers, including US Vice President JD Vance and billionaire Elon Musk, criticised the annulment of the elections, while the ambassadors of Germany, France, and the Netherlands expressed their support for the independence of the Romanian judiciary (Ilie & Charlish & Kerry, 2025). and supported the sovereignty of Romania's elections and decisions.

The consequence of the annulment of the elections due to Russian psychological-information influence was the blocking and removal of fake accounts, bots, and trolls. TikTok removed a "cluster" of accounts supporting the pro-Russian candidate Călin Georgescu, which violated the rules regarding unlabelled political advertising. Additionally, the platform deleted 66,000 fake accounts and 10 million fake followers before the elections (Financial Times, 2025)

This unprecedented event sparked a discussion on political campaigns on the internet, the use of AI, bots, trolling, and the spread of disinformation having a real impact on state politics, particularly on the eastern flank of NATO, in which Russia has an "interest" in interfering in public opinion and the selection of politicians favourable to its agenda.

In September 2025, Russia carried out the largest conventional attack on the territory of a NATO state since the beginning of the Russian aggression against Ukraine. Although since 2022 there have been regular Russian provocations in the form of violations of the airspace of countries on NATO's eastern flank, the drone attack that violated Poland's airspace was the largest military provocation. In addition to the conventional attack, Russia conducted a coordinated disinformation campaign aimed at placing the blame on Ukraine for the incident. The objective of this operation was to undermine trust in Poland's allies, destabilise relations between Poland and Ukraine, and also strongly destabilise and polarise Polish society.

Mainly digital disinformation mechanisms were used: frequently employed against Poland were fake news, bots, trolling, and in particular hate speech – mainly in the form of comments on social media. Russian propaganda sources spread narratives suggesting that the damage caused by the

drones was the result of an earlier storm, not an attack. It was also claimed that Ukraine had used "repaired Russian drones", pointing to the presence of duct tape on the wreckage as evidence. However, these claims were quickly debunked by photographic and video evidence, as well as witness testimonies and rescue services (DISA, 2025).

Additionally, a report by the organisation Res Futura (Jones, 2025) indicated an organised disinformation campaign in Polish social media, in which 38% of comments blamed Ukraine and 34% blamed Russia. The analysis showed that these narratives were the result of activity by pro-Russian accounts, aimed at undermining trust in the Polish government and NATO (Jones, 2025). The matter became so serious that it provoked a reaction from the Polish authorities. The Polish Deputy Prime Minister and Minister for Digital Affairs, Krzysztof Gawkowski, described the attack as "a planned provocation coordinated with a disinformation campaign" (Sonko, 2025). He emphasised that Poland has evidence confirming the intentional nature of the attack and the associated disinformation activities. In response to these events, Poland undertook actions aimed at protecting its sovereignty and the integrity of its democratic processes.

The case of Romania constitutes an example of the use of digital diplomacy and psychological operations by Russia in order to influence democratic processes in the countries of Central and Eastern Europe. The use of advanced digital technologies, social media platforms, and informational manipulation was aimed at supporting a pro-Russian candidate and undermining citizens' trust in democratic institutions. In response to these threats, Romania undertook actions aimed at protecting its sovereignty and the integrity of democratic processes.

PSYOPS automatically use the digital domain now. This is the reason for their propaganda and digital diplomacy tools to justify their aggression towards Ukraine, and also justify their influence which purpose is to divide the European Union.

The case of the drone attack on Poland in 2025 illustrates the use of digital diplomacy and psychological operations by Russia in order to influence democratic processes in the countries of Central and Eastern Europe. The use of advanced digital technologies, social media platforms, and informational manipulation was aimed at undermining citizens' trust in democratic institutions, trust in Poland's defensive capabilities, building antagonisms between Poland and Ukraine, fuelling already tense relations, in particular the waves of xenophobia that have recently been spreading through Polish society towards foreigners, especially those of Ukrainian and Belarusian origin residing on the territory of Poland.

References:

1. Alaphilippe, A., Gary Machado, G., Miguel, R., Poldi, F. (2022). Doppelganger – Media clones serving Russian propaganda. Disinfo. URL: https://www.disinfo.eu/doppelganger/

2. Blackburn, G. (2025). Romanian ministries accuse Russia of interference in Sunday's presidential runoff. Euronews URL: https://www.euronews.com/2025/05/19/romanian-ministries-accuse-russia-of-interference-in-sundays-presidential-runoff
3. Dumitrescu, R. (2025). Romania's cancelled 2024 presidential elections influenced by Russia, general prosecutor says. Romania-Insider.com URL: https://www.romania-insider.com/romania-cancelled-presidential-elections-russia-general-prosecutor-2025
4. Ertanowska, D. (2021). MEMES AS A MEANS OF COMMUNICATION AND MANIPULATION. Visnyk of the Lviv University. Series Journalism. 2021. Issue 49. P. 187–195
5. Ilie, L., Charlish, A., Kerry, F. (2025). Romanian court upholds measures against presidential election frontrunner in probe. Reuters URL: https://www.reuters.com/world/europe/romanian-court-upholds-measures-against-presidential-election-frontrunner-probe-2025-03-06/
6. Jones, M, G. (2025). Disinformation report misrepresented to claim Poles hold Kyiv responsible for drone incursion. Euronews URL: https://www.euronews.com/my-europe/2025/09/24/disinformation-report-misrepresented-to-claim-poles-hold-kyiv-responsible-for-drone-incurs
7. Marovic, I. (2018). The Path of Most Resistance. International Center on Nonviolent Conflict.
8. Pelin, M. (2025). Romania and the hybrid war.Radio România Internațional. URL: https://www.rri.ro/en/news-and-current-affairs/today-in-the-news/romania-and-the-hybrid-war-id928560.html
9. Russia Disseminates Disinformation Regarding Alleged Polish Drone Strikes. (2025). DISA URL: https://disa.org/russia-disseminates-disinformation-regarding-alleged-polish-drone-strikes/
10. Sonko, A. (2025). Russia deliberately attacked with drones, we have facts and evidence – Poland's deputy PM. The New Voice of Ukraine URL: https://english.nv.ua/nation/poland-russia-s-drone-attack-was-a-planned-provocation-with-disinformation-50544532.html
11. TikTok says it took down "cluster" of pro-Russian influencers in Romania (2025). Financial Times URL: https://www.ft.com/content/9c888f82-2e2d-44d4-ac1e-fcdbd830cec5?utm_source=chatgpt.com
12. Walker, S. (2025). 'These people are disposable': how Russia is using online recruits for a campaign of sabotage in Europe. The Guardian https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe
[1] Ma in Journalism and Social Communication UITM, European Academy of Diplopmacy: Executive Diploma in the Art of Diplomacy (EDAD). Media and Hybrid Warfare Specialist delfinaertanowska@gmail.com

DOI 10.69790/epis-rep-ird-1/27892