

RUSSIA'S CONCEPT OF INFORMATION CONFRONTATION, A DOUBLE-EDGED SWORD

Laurențiu-Leonard LĂZĂROIU

Joint Force Command Naples, Italy
laurentiu.lazaroiu@nato.int

Abstract: Russian information confrontation doctrine, a double-edged sword, encompassing cyber, propaganda, psychological operations, strategical messaging and forms of conventional sabotage, has focused its efforts in two directions, to adjust either internal domestic environment by securing the regime stability at home, or international democratic order by reshaping the offensive tools on its long-term power restoration strategy. To pursue its strategic objectives, the Kremlin utilizes information confrontation means alongside with other military and non-military techniques. The centre of gravity in the information confrontation consists in psychological effects and misleading in individuals' minds and perception, both domestically and in relation to international events.

Keywords: information confrontation, digital sovereignty, state control

1. Russia's information sphere

The Kremlin perceives total control over its domestic information space as a paramount tool for the national security, any insider vulnerability to the information space being seen as an ominous sign to Russian security. Related to that strategic approach, we convey that information sovereignty actions as a division of a more complex political concept- as long as digital sovereignty (tsifrovoy suverenitet) is seen as self-reliant and autonomous control of information and aversive to cyber intrusion. More complex than the Western concept of cyberspace, Russia is defining for its operational environment the term information space or information sphere. The theory is used with a positive connotation in a geopolitical protective pattern against foreign intrusion. To that, information space is becoming a perpetuation of Russia territorial state border, that has to be defended [1]. From the Russian doctrinal perspective, the information space includes the sum of activities to compile and to gather

information, as well as a large spectrum of elaborated attempts to influence individual and collective consciousness, affecting information infrastructure and including the center or meaning of information itself.

2. Digital sovereignty and the political control

From our analysis, we assume the disputes in the information space between Russia and Western countries would have an important asymmetric shape, as the Russia's adversaries, operating within open networks, would experience a state-controlled environment characterized by technical constraints, difficult to crack. Conversely, Russia, as a nation with a more closed network has the capability to operate under relative prerogatives. It is more than just the national government's ability to protect geopolitical national interests in the digital world, subordinated to digital sovereignty umbrella. The prerogatives allow an official strategy of alleged protection for the nation and includes elaborated psychological tools

for controlling Russians minds and actions. These tools are loyal to political orders. From a technical perspective Vladislav Bukharin (2016) links sovereignty explicitly to ownership, thus implicitly to internal control when defining technical components of Russian 'digital sovereignty', and identified the most used cyber tools by the Kremlin's apparatus [2]:

- Search engine (Yandex integrated Ecosystem: Yandex apps, Yandex Taxi, Yandex Music, and Yandex Translate)
- Social media platforms (Yandex, Vkontakte, Odnoklassniki);
- Domestic operating system and software (Astra Linux, Kaspersky Lab;
- Microelectronics (Mikron);
- Networking equipment (Nerpa, JSC Rostelecom,);
- National segment of the Internet (Ru Net);
- Payment system (Mir, SPFS);
- Cryptographic algorithms and protocols.
- Navigation systems.

It is becoming obvious that the absolute situation would embrace autonomous Internet infrastructure, a unifying ideology subordinated to the political values, a dense ideology in response to international sanctions, and subordinated mass media surrounded by a powerful legal system. Russian Internet (RuNet) as an important ingredient of digital sovereignty, known as a controlled Internet capability, made of popular research engines and social media sites, has permitted Kremlin to influence Russian minorities among neighboring countries, widening the sphere of influence also in the digital environment. However, Russia's growing effort in having its own detached Internet mitigates the national advantage of RuNet, as outside their borders it will narrow their managing capacity and capabilities.

3. The grey zone, between internal and external interference

To interfere with the Western democracies, on the information confrontation theater,

The Russian Federation has employed two types of operations, including large scale of means: technical measures like cyber operations and psychological measures with the aim to influence, disrupt, and usurp the adversary's morale and decision-making process.

3.1 Technical measures

Starting from state ownership over cyber components reality, we added Kukkola's perspective including his analyzes on several tools that Russia is employing on the effort to control and nationalize the domestic information infrastructure [7]. Finally, we appreciated as comprehensive measures, both for national deterrence and for internal censorship purpose, the spectrum of actions conducted by the Russian state' actors, as follows:

- Scientific research for development of Russian national technological equipment, either hardware or software, delivered to security and military structures;
- Employment of State encryption and authentication equipment to protect the systems against foreign interference and intrusion;
- Development of tools for blacklisting and content control to remove or restrict website access;
- Telephone and Internet tracking, not just a metadata level, but also content and traffic. It naturally affects foreign nationals travelling to Russia. Telecommunication service providers are required to set up probes in their network systems, connected to the Russian Security and Intelligence Services;
- Expansion of centralized surveillance systems and data traffic localization have as objectives counterintelligence, law enforcement and political control purposes. State surveillance mechanisms are augmented by automatic video and audio networks, by enabling high-speed collecting and use of AI for a large spectrum of objectives, including stifling dissents,

- Law enforcement efforts for Critical information infrastructure protection. The legal obligation for internal actors to protect it, sometimes through disconnection from the global network. All the measures encompass robust and extensive regime control;
- Employment of electronic sovereignty and information sovereignty measures. Technological and psychological control of domestic environment by state-controlled news services, patriotic and religious institutions affiliated to Russian intelligence and security services for state-controlled propaganda [5];
- Evolution of the management capabilities, including AI tools, for processing informational flow and providing feedback through real-time reactions to imminent threats.

3.2 Russian legal framework regulating information sphere

The Russian political regime created specific laws for two main reasons: to “collectivize” the critical information infrastructure against external actors and secondly directed on monitoring data flow from the internal Internet. The spectrum of laws and regulation created for effective control started on 1998, the government adapted Soviet era surveillance technology, known as the System of Operative-Search Measures (SORM), for the digital domain. In the early 2000s, Kremlin implemented a legislation that de facto: ban criticism of the government, permit unrestricted surveillance of citizens, monitor online behaviors, and increase state control on cyber domain [2]. Since 2012, just after Putin’s return to Kremlin, Russia firmly has started their national cyber security program, GosSOPKA, a state shield system for identifying, precluding and eliminating the consequences of cyber-attacks on critical infrastructure. To support this initiative, Kremlin has adopted several strict, centralized control laws. The most relevant are:

- Internet censorship, 2012 State Duma passed 139-FZ, implements a central Internet ban facility, control by the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications-Roskomnadzor. Next year, in 2013 legal revisions allowed the blocking of content suspected "in terrorist activities", "calls for riots", "inciting hatred" and any other actions "conducted in violation of established procedures" [9];
- In 2014, government decree 758, on phone number provision for wi-fi. Public wi-fi users must provide their phone number. To buy a sim card an ID is requested, so this law makes it impossible for a sim card owner to browse anonymously on Internet;
- In 2016, the so-called Yarovaya amendments, 374-FZ and 376-FZ demanded telecommunication providers, social media online platforms, and messaging services to save users data for three years and permit the FSB access to users’ metadata including encrypted files, without court order;
- In 2017, Vladimir Putin ratified 276-FZ which outlaws all software and websites related to bypassing the Internet filtering system in Russia, including proxy-services and virtual private network (VPN) services;
- Since 2019 Russia has required the installation of specific software that can monitor online traffic and authorize to cut the Federation off from the global Internet – Sovereign Internet law, 90-FZ. From 2019 to 2024 Russia introduced new amendments and regulatory actions aimed at narrowing online freedom of movement, tightening state control, and isolating RuNet from global Internet;

Legal framework adopted by the state since Putin’s return to the presidency, are officially aimed at regulating information space but to facilitate digital authoritarianism — the use of cyber technology by the Russian authoritarian

power to surveil, persuade, repress domestic anti-system activities and to manipulate foreign populations.

3.3 Psychological operations

Complementary to targeted campaigns to destabilize the West through multiple attempts of undermining NATO and democratic governments and their election campaigns, Kremlin has promoted the narrative of Russia as a reliable and resourceful ally as a beneficial alternative for non-Western countries. Without any doubt the purpose was to enhance its international stance, followed by regional influence [6]. Psychological operations focused either on reshaping or totally changing on enemy's perception are not restricted to the virtual world. Before the Internet and AI capabilities being on war, state actors employed television, radio and newspapers to conduct information operations, of course, at a lower scale, but against a less educated target. Overall, the purpose remains the same, to change enemy's perception with the aim of achieving strategic objectives. As modern world has become more dependent on digital infrastructure, all nations have exploited reliance on cyberspace, with sophistication and precision. The targeted campaigns against the West have involved flooding the information sphere with elaborated and conceived tactics to create political doubts, conspiracies, contradiction and chaos oppressing the efforts of separating objective truth from delusion. Russia on its power restoration objectives has become adaptive and innovative, operating a vast arsenal of instruments, establishing methods and techniques connected to the modern technological rhythm and to the geopolitical reality. Thus, the goal is a full-time manipulating pressure, before, during and after a conflict, directed at the enemy's perception of reality [8]. During the conducted research timeframe, analyzing open sources reports, interviews with the western stakeholders, political actions and geopolitical events, we identify a large

spectrum of tools, much more efficient with the AI algorithms. AI works like a catalyst for processing and creating audio and visual content with great impact, the strategies focused on jeopardizing adversaries' information environment and strengthening Kremlin's information sphere. During recent years, forgery, especially the presentation of artificially created information, with no connection to real facts, but presented as it were, became an efficient instrument to dismiss accusation and to fabricate reality. Identified spreading groups for Kremlin's loyal reality consist of:

- existing state-controlled media outlets subordinated to the political ecosystem;
- the compulsive use of national and historical narratives;
- the use of religion as a pillar to the political warfare influence campaign.

Moscow often seizes the opportunity to exploit the societal divisions, even for events emerged independent of Russian sphere of main interest-as observed during the Yellow Vests protests in France, the Black Lives Matters movement in the USA, COVID-19 conspiracy theories, migration in Europe etc. Analyzing Russian Informational Confrontation Doctrine we can identify two main strategies, embedding a large spectrum of complementary instruments for the same goal:

- the use of active measures conducted for the clear purposes of cultivating pro-Russia ideological sentiment;
- the reflexive control techniques to obtain the same result.

Reflexive control consists in more elaborate information warfare that seeks to redefine the enemy's perception, motivations and goals through disinformation, psychological operations to match the adversary's decision with Kremlin's objectives, while believing those decisions are their own.

Technically speaking, the reflexive control's main purpose is to offer to the enemy your choice and to be perceived like his own independent decision. By flooding the information space with conspiracies,

emotionally charged content produced by generative AI, deepfakes and tailored messaging to specific audience, Russia tries to paralyze institutions, democracy and decision makers.

4. Conclusions

The efficiency of Russian disinformation, internet troll attack and smear campaigns is represented by unexpected strikes, characterized by deficiencies on cognitive bias, social media bias and human emotions. Adding the surprise effect and the time pressure we have the ingredients for delivering shocks and an overall negative impact to democratic institutions' reputation and credibility. Isolated, small countries, to resist to Kremlin's influence operating (i.e. Baltic states, Moldova) must apply pragmatic strategies with efficiency in regards of limited resources' allocation. For European Union members, such strategies are based on comprehensive and integrated defense concept -to protect not individually, but together. The Kremlin demonstrates its readiness, and its influence is reflected in top

polls across Europe's major capitals. For 2026, the political elections in France, Germany, Hungary, Slovenia offer Moscow a framework with large scale of opportunities to disrupt democratic process, primarily by supporting populist parties that share a sympathetic stance toward Kremlin's regime, as well as concealed and unexpected tactics by amplifying divisions among Western allies. As a protective measure, the European Union has enacted legal constraints which should impose obligations on social media platforms to ensure accuracy and transparency of their data to protect the users, including from harmful and illegal content. Thus, the UE regulatory framework has improved, but is not filling all the gaps, placing greater responsibility on member states to strengthen regulations (i.e.: Digital Services Act- entered into force in 2022; Artificial Intelligence Act- in 2024). We expect Russia to deploy subversive tactics and harness AI generated content to influence election outcomes and undermine trust in European Union and NATO.

References

- [1] Kukkola, J., Ristolainen, M. Projected territoriality: A case study of the infrastructure of Russian 'digital borders'. 2018. https://www.researchgate.net/publication/326292919_Projected_territoriality_A_case_study_of_the_infrastructure_of_Russian_'digital_borders'. Accessed: March 3, 2026.
- [2] Bukharin, V. Vladislav. The Russian's Digital Sovereignty as a Technical Basis of Information Security. MGIMO Review of International Relations. 2016; vol.51(6): pp.76-91. Available at: <https://doaj.org/article/aac6b1d404b249d3888fabd5b9598f5e>. Accessed: February 16, 2026.
- [3] Hakala, J., Melnychuk J. Russia's strategy in Cyberspace. NATO Cooperative Cyber Defence Centre of Excellence. Riga, 2021.
- [4] Bambals, R., et al. Handbook on Countering Disinformation: Recognize and Resist. Second edition, State Chancellery of the Republic of Latvia, 2025.
- [5] Schafer, B., et al. The Russian propaganda nesting doll, Alliance for Securing Democracy, May 2024, pp. 10-27.
- [6] Barratt Dewey, O., Hydra Warfare: The GRU in Russia's Shadow War Against the West, King's College London, 2024.
- [7] Polyakova, A., Meserole C., Exporting digital authoritarianism: The Russian and Chinese models. Foreign Policy, The Brookings Institution. 2019. Available at: [Exporting digital authoritarianism: The Russian and Chinese models](#). Accessed: March 5, 2026.

- [8] Soldatov, A., Borogan, I.. The New Iron Curtain. 2022. Available at: <https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/>. Accessed: February 9, 2026.