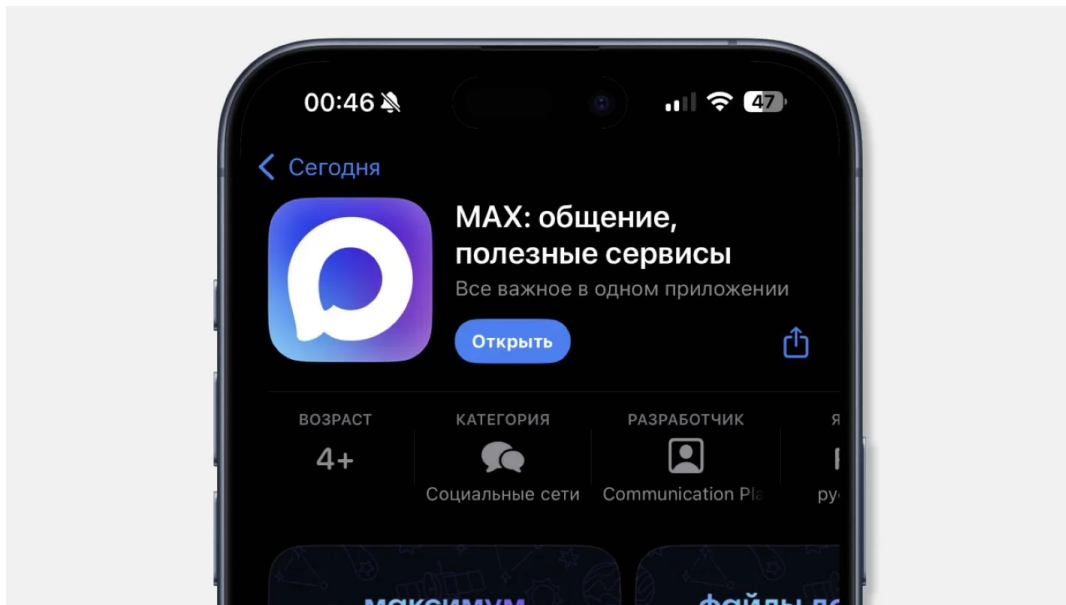




Russia: why the WhatsApp block is (also) a measure of Cognitive Warfare

Published on 14/02/2026

Cognitive warfare is not “just propaganda”. In the [most common euro-atlantic interpretation](#), it is the set of operations (informative, psychological, and technological) aimed at **influencing perceptions, decisions, and behaviors**, eroding trust, rationality, and social cohesion: a domain where the target is not (only) the infrastructure, but **the mind**. NATO describes it as a competitive ground that “attacks and degrades rationality” and increasingly involves non-military targets. In Italy, a [Ministry of Defense dossier](#) places the phenomenon within a “whole of government” response, meaning transversal and coordinated among defense, intelligence, institutions, and society.

If this is the framework, the article you reported on the WhatsApp block in Russia and the push towards the “Max” app (VK) becomes an almost textbook case: not because it demonstrates “a manipulation campaign” in the classic sense, but because it shows **how control of the digital ecosystem** (platforms, data, communication channels) can be used to gain an advantage in the

cognitive dimension: reducing citizens' informational autonomy, increasing the traceability of social networks, and, in perspective, making selective censorship and narrative orientation easier.

What is *cognitive warfare* (and what distinguishes it from “classic” disinformation)

The substantial difference between traditional disinformation and *cognitive warfare* lies in the **scale leap**:

- **Objective**: not just to convince about a fact, but to *shape* the mental context (trust, emotions, sense of belonging, perception of legitimacy).
- **Means**: beyond content (posts, media, influencers), **digital architectures** matter: which apps you use, which feeds you see, what voice notes you can send, how secure a chat is, who controls servers and metadata.
- **Strategic advantage**: when the State manages to “govern” the communication ecosystem, it reduces the cognitive resilience of the target society (or, internally, neutralizes dissent and pluralism).

Put brutally: *if you control the channels, you also control the conditions in which ideas and social organization circulate.*



Russia: why the WhatsApp block is (also) a measure of Cognitive Warfare

The WhatsApp block: a “platform” action with cognitive effects

According to international sources, on February 12, 2026, Russia **blocked WhatsApp** and, through official statements, directed users towards **MAX/Max**, a state-supported alternative. This move has at least three implications consistent with the logic of *cognitive warfare*:

1. Reduction of mass effective privacy

Various journalistic reconstructions highlight that Max is presented as a “super-app” and is criticized for features considered more favorable to surveillance, including concerns about encryption and authority access.

2. Dependence on domestic infrastructure

The forced exit from a global platform (Meta) in favor of a national platform shifts **data, digital identities, and relationships** within a perimeter more controllable by Russian authorities and regulators.

3. Closure of the “attention market”

If the average user communicates, pays, accesses services, and receives notifications within a single ecosystem (super-app style), then the State can more easily intervene on *visibility* and *priority* of information: it is not necessary to convince everyone, just make it harder to coordinate, inform, or bypass blocks.

The block within a broader project: Runet and “sovereign internet”

Runet is a Russian project for a more autonomous/isolatable network. This trajectory is compatible with the normative and technical evolution of the so-called “**Sovereign Internet Law**” of 2019, which grants Roskomnadzor and the State tools to centrally manage traffic and, in declared “threat” scenarios, even isolate the Russian segment.

Over time, analyses by NGOs and observers describe the implementation through devices like **DPI / TSPU** (traffic filtering and inspection) that make it easier to block or slow down services and protocols.

Here lies the key connection with *cognitive warfare*: **it is not just censorship** (removing content), it is **control of communication conditions** (who can talk to whom, with what

security, at what cost, with what alternatives).



The Russian measures to highlight (reasoned chronology)

To compare “cognitive warfare” and the “WhatsApp/Max case”, the most concrete part is the measures that make forced platform replacement possible:

- **2015 - Data localization:** Russian law requires that the personal data of Russian citizens be stored on databases in Russia; this becomes a recurring lever against foreign platforms.
- **2019 (effective from November 1, 2019) - “Sovereign internet”:** law and implementing regulations strengthen centralized traffic management, with technical obligations for operators and powers to Roskomnadzor in case of “threat” to network stability/security/integrity.
- **2021 - Preinstallation of domestic software:** the obligation to sell devices with preinstalled Russian software/apps comes into force, consolidating a “default” channel towards national services.
- **From 2022 - Crackdown on Western platforms:** after the large-scale invasion of Ukraine, Russia expands blocks and restrictions on Western social networks and services (Facebook/Instagram and others), with a more aggressive regulatory climate.
- **2025-2026 - Push to Max + targeted blocks:** February 2026 news describes the complete block of WhatsApp and, in parallel, pressures and limitations on Telegram; the explicit political direction is to migrate users to Max.

In this context, “mandatory Max” should be read as a **continuation** of the Russian policy of preinstalling domestic software: a mechanism that drastically lowers the adoption threshold of national alternatives and makes every subsequent block more effective.

Final comparison: *cognitive warfare* vs WhatsApp block

Cognitive warfare describes the objective: to influence perceptions and behaviors, exploiting cognitive and social vulnerabilities.

The WhatsApp/Max case shows the “infrastructural” method: instead of fighting only on the content level, it acts on:

- *access point* (apps and store, preinstallation, “system” alternatives);
- *rules of the game* (data localization, compliance obligations, block threats);
- *network technology* (throttling/selective blocking capability via DPI and centralized management).

In other words: **the WhatsApp block is not automatically “a cognitive warfare operation”**, but it is a measure that **creates a more controllable informational environment**, and thus *enables* (or makes cheaper) strategies of influence, surveillance, and censorship. It is the difference between “persuading” and “designing” the ecosystem in which persuasion (or repression) becomes easier.

News link: <https://www.theguardian.com/world/2026/feb/12/russia-attempt-block-whatsapp-meta-says>