

Words and Weapons: Disinformation and Technology in Russia's War Against Ukraine

Nataliia NECHAIEVA-YURIICHUK

Abstract: *Amid the rapid development of digital technologies and AI, Russia is increasingly combining technological progress with information manipulation in its war against Ukraine. This article attempts to analyse how the Russian Federation is transforming technological development in the military sphere into a means of promoting propaganda narratives. Using the deployment of the Russian "Rassvet" satellite constellation as an example, the author examines how military technology development is becoming a tool for disinformation and propaganda, and how the Russian system for producing and disseminating disinformation operates on a global scale.*

Keywords: *Russia-Ukraine war, hybrid war, disinformation, propaganda, satellite technologies, AI.*

Russia launched a war against Ukraine in 2014 when it occupied the Autonomous Republic of Crimea and parts of Ukraine's Donetsk and Luhansk regions. It was then, in 2014, that the world gained a new appreciation for the significance of words (in the context of information) and their direct connection to security – from the individual to the nation and the continent. The very beginning of Russia's war against Ukraine was the launch of a series of measures – primarily informational and military-political – aimed at creating a distorted perception among the international community regarding the events in Ukraine.

The Armed Forces of the Russian Federation crossed Ukraine's state

border on February 20, 2014. On that day, military trucks without identification marks began appearing in the Ukrainian Crimea, and soldiers in Russian uniforms – also without identification marks, known as the "little green men" – were spotted at strategic sites. The very next day, February 21, following the flight of then-President of Ukraine Viktor Yanukovich from Kyiv, Russia launched a military operation to seize the Autonomous Republic of Crimea. Just one week later, on February 27, Russian special forces seized the buildings of the Verkhovna Rada and the Council of Ministers of Crimea. The Russian occupation authorities proclaimed Sergey Aksyonov "head" of Crimea and began preparations for

a sham referendum¹. The Russian authorities denied the very fact of a Russian presence in Ukraine's Crimea, attempting to paint a picture of a civil war in Ukraine and publicly referring to their troops as "self-defense forces" allegedly formed by residents. On February 28, after Russian troops seized the Simferopol airport, Russian Ambassador to the European Union Vladimir Chizhov told Euronews: "There are no troops there at all, at least not Russian ones," echoing Moscow's official line. When asked by Bloomberg, Russian President Vladimir Putin even suggested: "Go to a store here, and you can buy any uniform there."² It was only after the so-called referendum in Crimea that Moscow acknowledged its presence and involvement in the armed seizure of Crimea. Symbolically: Moscow established the "For the Return of Crimea" medal long before the so-called referendum on the peninsula. The medal bears the date February 20, 2014 – the date the Russian special operation began, marking the start of Russian aggression³. A year later, in 2015, Vladimir Putin admitted that he himself had given the order to launch the operation in Crimea⁴.

Since then, a number of changes have taken place both in the geopolitical landscape and in the nature of warfare, its tools, and the technologies employed. What has remained constant is the mandatory use of information and hybrid warfare tools to influence the consciousness and

worldview of broad segments of the population in various corners of the globe.

This research paper is an attempt to analyse how Russia exerts psychological influence on target audiences and the general public by combining real and fabricated technological narratives to advance its own agenda – specifically, to weaken support for Ukraine and normalise the international community's attitude toward itself. The analysis is based on publications in open sources, analytical reports, and journalistic investigations, since objective information about the "Rassvet" project and the mechanisms of its narrative exploitation is restricted, and open sources remain the only available way to track these processes and analyse them in real time. Furthermore, with the advent of AI, developments in the field under study are so rapid that they can be tracked through observation and documentation in open-source formats.

According to analysts at the Royal United Services Institute, 2026 was a year of "hybrid escalation by Russia," in which weaknesses on the front lines were actively offset by sabotage and influence operations⁵. Russia continues to target Ukrainian and Western audiences separately, while simultaneously making extensive use of generative models to produce deepfakes, AI-generated "witnesses" to events, and networks of mirror sites, overwhelming the fact-checking community with a deluge of fakes and disinformation. In an effort

to amplify its destructive influence on public opinion, Russia is actively using AI to spread disinformation. To this end, it employs a technique of “poisoning” Large Language Models (LLMs) by generating fake websites, news portals, and pseudo-analytics, which are systematically “fed” to algorithms through SEO optimisation. The main goal is to reproduce the Kremlin’s disinformation messages about Ukraine – and beyond – in responses to audience queries by bots such as ChatGPT, Gemini, Claude, and others⁶.

Russian disinformation networks began forming as early as 2014, with Olginio; however, until 2022-2023, the networks producing disinformation required human involvement in creating and disseminating content. The emergence and rapid development of AI changed the situation – now neither actors nor directors are needed to generate fake videos. Moreover, producing fake content is accessible to virtually anyone, not just states with significant resources. Among the most well-known Russian disinformation networks today is “Storm,” which, in various forms, produces a wide range of content to promote Kremlin narratives. For example, “Storm-1516” specialises in videos presented as coming from “whistleblowers” and pseudo-journalists, while “Storm-1679” produces pseudo-documentaries in the style of American investigative reports⁷.

In response to the technological advancement of Russia’s disinformation machine, the democratic world is

developing its own technological defences, among which, in our view, the availability of objective expert information in various languages on open platforms and sites (Common Crawl) to prevent or minimize the “poisoning” of AI by Russian propaganda and disinformation, to fill information gaps regarding Ukraine and the Russian-Ukrainian war, and so on is critical.

The war currently being waged for the information space is extremely aggressive. It runs parallel to the combat operations on the front lines of the Russia-Ukraine war and combines the technological and disinformation dimensions of the latter. The combination of conventional and unconventional means of warfare is known in academic discourse as hybrid warfare, the basic definition of which was formulated by Frank Hoffman:

Hybrid war is the war which “incorporates a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder”⁸.

Hoffman’s concept served as a starting point for further research into hybrid wars in their various forms, including Russia’s hybrid war against Ukraine. With the unfolding of Russia’s war against Ukraine, Ukrainian scholars are increasingly focusing their attention on research into hybrid warfare, its forms, and its tools. Among them is Yevhen Magda, director of the Institute of World Pol-

icy. In his works, the scholar emphasises:

“Hybrid warfare is the attempt by one state to impose its political will on another (or others) through a combination of political, economic, and informational measures, without declaring war, in accordance with the norms of international law”⁹.

The experience of the Russian-Ukrainian war demonstrates that the set of measures is constantly being refined and expanded in the context of technological development. What remains constant is the desire of a single state to impose its will on others using hybrid tools.

The Kremlin’s approach to understanding the nature of hybrid war differs significantly from those outlined above. While Western discourse treats hybrid war primarily as an analytical category for classifying external threats, Russian discourse presents it either as a civilizational conflict of values (the West versus Russia) or as a geopolitical struggle for global dominance. In both cases, Russia is portrayed as the victim, not the aggressor. Moreover, Russian public debates on hybrid warfare and hybrid threats “can be seen as a part of Russia’s strategic communications to the extent that the debate amplifies officially accepted vision of threats towards Russia”¹⁰. At the same time, Russia itself is actively using hybrid influence tactics to secure victory in the war.

Manipulation, deception, and the falsification of facts to support Russia’s self-justifying narratives can

also be observed in technological applications, particularly in the field of armaments. In modern warfare, satellite internet plays a crucial role not only in ensuring communications but also in data exchange and other military operations. As early as 2017, the Kremlin attempted to launch a satellite communications system (“Efir”). However, a year later, it was removed from the program because no private investors were found willing to fund its launch. In 2018, the creation of the “Sfera” project was announced, which was intended to include the aforementioned “Efir” as well as other satellite systems, including “Megafon 1440.” The latter emerged in 2020 as a project of the mobile operator of the same name. At the end of 2021, “Megafon 1440” began transforming into a separate company tasked with developing and manufacturing satellites, ground infrastructure, and other key system components. When it became clear in 2022 that the ambitious plans to launch hundreds of satellites into orbit would not be realized, this project – now known as “Bureau 1440” – became a key player in the field of low-Earth orbit satellite internet¹¹.

In June 2023, the first three experimental satellites of the “Bureau 1440” mission, part of the “Rassvet-1” program, were launched into orbit. A year later, three more – full-scale prototypes of production satellites – were launched as part of the “Rassvet-2” mission. After losing access to Starlink in February 2026, the Russians accelerated their work in this

area¹². In March 2026, the company launched its first group of 16 satellites, and by the end of July, it announced that it had placed a second group of satellites into orbit¹³. Looking ahead, Moscow plans to significantly increase the number of satellites – specifically, to more than 250 over the next year. If the Kremlin's ambitious plans are realised, the “Rassvet” satellite constellation could pose a new threat: an increase in “communication windows” – the time during which a Russian satellite is within Ukraine's coverage area and can provide communication for UAV control. And if scaled up, this time could expand to continuous coverage, creating new challenges for countering Russian drones¹⁴.

However, even with the accelerated deployment of the “Rassvet” satellite constellation, it is still too early to speak of a full-fledged competitor to Starlink. The key question today is: Can Russia expand its satellite constellation quickly enough and support it with ground and launch infrastructure? This requires not only a sufficient number of satellites but also the ability to launch them into orbit on a regular basis: for the 250 satellites planned for 2027, at least 15 rocket launches will be necessary¹⁵. And in the coming years, according to a Roscosmos representative, demand for Soyuz rockets will exceed the Progress plant's production capacity by 50%¹⁶.

Experts currently do not have a unified position on assessing the system's combat readiness¹⁷.

However, the threats posed by this project – not only to Ukraine – are evident to the European Union as well. In July 2026, the 21st sanctions package was approved, which included the “Rassvet” system as «the manufacture of a system that Russia is developing as an alternative to Starlink». As Senior Fellow at the Bruegel think tank Jacob Funk Kirkegaard said, “Denying Russia the capability... over time, to establish an alternative to Starlink would obviously be a very important priority”. He also underlined, that “As the EU or Europe more broadly prepares for a world in which we have to deter Russia on our own for the long run, denying Russia their military capabilities in the next three, four, 10 years from now is very important for our own security”¹⁸.

At the same time, the Russian side is actively promoting the combat capabilities of the “Rassvet” and its technological potential through its own network of media outlets, thereby – in the author's view – attempting to influence public sentiment and assessments of Russia's capabilities in the Russian-Ukrainian war. A telling example in this case is an article “The Landlord Lost the Keys: Russia's War Gamechanger in Low Orbit” published on SouthFront online resource. In the article, “Rassvet” is positioned as «a crowbar prying open the padlock on low Earth orbit, and the door is already swinging wide over Ukraine»¹⁹. It is worth noting that the propaganda in this article operates primarily not at the

level of basic facts – which are easy to verify (the launch dates of the satellites, their number, etc.) – but at the level of tone and metaphorical framing. This article is a paean to Russian technology, for which – according to the unnamed authors of the piece – governments, “fearing ‘colour revolutions’» are already lining up for it²⁰. Metaphors, allegories, and emotional appeals – alongside statistics (the planned 250 satellites by mid-2027) – serve an affective function and are intended to instill in the audience a sense of inevitability and powerlessness in the face of the Kremlin’s “technological superiority.” Thus, in our view, the main goal of Russian propaganda is achieving in such a way – it is spreading fear regarding the Russian Federation’s military and technological capabilities and aimed to reduce support for Ukraine, since in democratic societies, elections are the primary instrument of democracy and determine a country’s domestic and foreign policy course.

Although SouthFront positions itself as an independent analytical resource, it is officially subject to sanctions imposed by two independent jurisdictions. The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury added SouthFront and NewsFront to its sanctions list in 2021 for activities carried out on behalf of Russian intelligence agencies²¹. The European Union made a similar decision in 2025, adding the platforms NewsFront and SouthFront to its sanctions list; both outlets present distorted

interpretations of history and manipulated information in line with Kremlin messaging while also targeting European and global audiences with distorted and manipulated information²².

Publishing information on this website is dangerous not so much because of the website’s audience as because regional and local media outlets in various countries systematically translate and republish the content under the guise of independent local journalism. Indeed, a recent study in Romania found that: the single largest source of News Time Romania’s (NTR) TikTok content is SouthFront, a Russian-linked outlet that produces battlefield updates, casualty reports, and geopolitical commentary supportive of the Russian Ministry of Defence. Of the 788 TikTok posts, 270 (or 34.3 percent) consist of „SouthFront,, articles translated into Romanian and accompanied by direct links to southfront.press or its Telegram account. On Telegram, SouthFront citations exceed 2 766 instances, making it the fourth most cited source overall behind three domestic Romanian outlets („ActiveNews”, „R3media” and „Ortodoxinfo”) which operate within Romania’s borders but are within the Kremlin-aligned media ecosystem²³.

SouthFront is one of the content sources for the Russian propaganda network “Pravda” (Portal Combat), an automated ecosystem of aggregator websites that republish content from other sources, ranging from Russian state media to social media

and Telegram channels. According to the study DFRLab, the top five sources mentioned in Pravda articles are the Russian news organizations TASS (136 000), RIA Novosti (99 000), Lenta (89 000), Komsomolskaya Pravda (59 000), and the government-owned RT (54 000). Other cited news outlets included the Russian TV channels Ren.tv and Tsargrad. Many of these outlets have been restricted or sanctioned in the United States, Canada, and the EU²⁴. Through this network, content published on overtly propagandistic and sanctioned websites (such as SouthFront) loses its direct trace of origin as it passes through an automated translation and republishing system and appears to the reader as a seemingly independent publication in their native language from a familiar source.

In addition, this network is actively used for AI poisoning or LLM grooming. Functioning as an “information laundry,” this network poses as an authoritative source and poisons AI tools and even Wikipedia, primarily on topics related to Russia’s war against Ukraine²⁵. As a direct result, when users ask AI-powered chatbots that rely on large language models (LLMs) trained on sources such as Wikipedia, they receive pro-Kremlin, anti-Ukrainian content in response. According to the author’s observations, users of AI-generated content increasingly note that the AI cites Wikipedia articles as sources.

According to the study’s findings by Anthropic, the UK AI Security

Institute, and the Alan Turing Institute, it takes as few as 250 malicious documents to compromise the answers of even very large (13B parameters) and highly capable models. Once this harmful content has been baked into a model’s weights, the only fix is a full (and extremely expensive) retrain²⁶. The “Pravda” network publishes thousands of articles every day. Thus, in today’s digitised and automated information space, a single piece of disinformation can reach millions of people on different continents – both directly, through reading the content, and indirectly, through interactions with AI chatbots without proper verification of the information and sources.

The analysed “Rassvet” project illustrates how, in the current war against Ukraine, Moscow not only constructs a distorted worldview based on its own propaganda and disinformation narratives but also entrenches it in the minds of digital content consumers using modern technologies. This same logic is applied to other types of weaponry, with claims about their power and invulnerability aimed primarily at intimidating Western and Ukrainian audiences, spreading panic, and reducing or eliminating support for Ukraine in the face of “invincible Russia”²⁷.

At the same time, Moscow is creating and spreading blatant disinformation claiming that Ukraine allegedly possesses or is developing weapons of mass destruction – primarily biological weapons – that are

prohibited under international law. Among the most striking examples is a statement made in October 2022 by Vasily Nebenzya, the Russian Federation's Permanent Representative to the UN, claiming that biological laboratories are allegedly operating in Ukraine where U.S. biological weapons are being developed and the potential for spreading dangerous infections via migratory birds is being studied. At the same time, claims were made about so-called "combat mosquitoes" that had been trained to attack soldiers of the aggressor state and infect them with various diseases²⁸. It is worth noting that Russia began spreading the disinformation narrative about American biolaboratories as early as 2010, and since then it has been systematically updated and repackaged for various audiences.

In summary, it is worth noting that in its war to preserve its empire at Ukraine's expense, Russia actively utilises modern technological capabilities both in weapons development and in information warfare. Its logic is that any fact – whether real (new types of weapons) or entirely fabricated ("combat mosquitoes") – is subordinated to the goal of exerting psychological influence on the target

audience in order to advance the Russian agenda. Specifically, this aims to reduce or eliminate support for Ukraine by instilling fear of a stronger Russia or of Kyiv's "uncontrollability" – a Kyiv that is "developing" biological weapons and "training mosquitoes" to "attack people based on their ethnicity or nationality". And despite the sheer absurdity of this last claim, the lack of skills in verifying information in a world where artificial intelligence is actively used could lead to the normalisation of such narratives in the public consciousness – which is exactly what the Kremlin is counting on.

Countering Russia's hybrid war requires new mechanisms to protect the information space – mechanisms relevant to individual consumers of digital content, on the one hand, and the architecture of AI technologies, on the other. The latter reinforces the need for systematic attention from governments and civil society to developing media literacy and critical thinking skills among the population, as well as intensifying efforts to generate objective information – especially regarding the Russia-Ukraine war – and to use networks containing objective information to train LLD.

Notes

¹ 20 лютого: початок окупації Криму і війни Росії проти України, 2025, <https://crimea-platform.org/news/20-liutoho-pochatok-okupatsii-krymu-i-viynny-rosii-proty-ukrainy/>, (accessed 23.08.2026).

² Від «Їх там немає» до «Що приховувати?»: як Росія заперечувала, а потім визнала захоплення Криму, 2019, <https://www.radiosvoboda.org/a/krym-putin-rosijski-vijskovi/297920-92.html>, (accessed 24.08.2026).

- ³ Кислиця в ООН: Росія вигравіювала на медалі дату початку агресії проти України, 2021, <https://unn.ua/news/kislitsya-v-oonr-osiya-vigraviyuvala-na-medali-datu-pochatku-agresiyi-proti-ukrayini>, (accessed 24.08.2026).
- ⁴ Від «Їх там немає» до «Що приховувати?»: як Росія заперечувала, а потім визнала захоплення Криму, 2019, <https://www.radiosvoboda.org/a/krym-putin-rosijski-vijskovi/2979-2092.html>, (accessed 24.08.2026).
- ⁵ Російська дезінформація у 2026 році: нові кампанії та інструменти, 2026, <https://www.united-ukraine.org.ua/post/russian-disinformation-in-2026-new-campaignsand-tools>, (accessed 24.08.2026).
- ⁶ Російська дезінформація у 2026 році: нові теми та інструменти. Аналітична доповідь, 2026, <https://www.united-ukraine.org.ua/post/russian-disinformation-in-2026-new-topics-and-tools>, (accessed 24.08.2026).
- ⁷ Баловсяк Н. «Шторм-1516» та інші: як Росія створила глобальну екосистему інформаційного впливу, 2026, <https://tyzhden.ua/shtorm-1516-ta-inshi-iak-rosiia-stvoryla-hlobalnu-ekosystemu-informatsijnoho-vplyvu/>, (accessed 24.08.2026).
- ⁸ Franc G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007, p.29.
- ⁹ Є. Магда, *Гібридна війна: вижити і перемогти*, Харків, 2015, p.4.
- ¹⁰ Pynnöniemi K., Jokela M. Perceptions of hybrid war in Russia: means, targets and objectives identified in the Russian debate, 2020, <https://www.tandfonline.com/doi/epdf/10.1080/09557571.2020.1787949?noredirect=true>, (accessed 24.08.2026).
- ¹¹ Пилипів І. Росія втратила Starlink і буде замінювати. Що відомо про систему "Рассвет", Економічна правда, 2026, <https://epravda.com.ua/svit/rosiya-rozvivaye-vlasniy-suputnikoviy-internet-zagroza-dlya-ukrajini-8-24130/>, (accessed 24.08.2026).
- ¹² Росія прискорила будівництво власного аналогу Starlink, 2026, <https://newformat.info/socium/rosiia-pryskoryla-budivnytstvo-vlasnoho-analohu-starlink/>, (accessed 24.08.2026).
- ¹³ І. Пилипів, *op. cit.*
- ¹⁴ І. Моляр, Це вкрай небезпечно для нас: Грабський про угруповання російських супутників "Рассвет", 2026, <https://espreso.tv/viyna-z-rosiyeyu-tse-vkray-nebezpechno-dlya-nas-grabskiy-pro-ugrupovannya-rosiyskikh-suputnikov-rassvet>, (accessed 24.08.2026).
- ¹⁵ А. Крупка, Росія створює альтернативу Starlink: чи зможе Україна її зупинити, 2026, <https://tyzhden.ua/rosiia-stvoriue-alternatyvu-starlink-chy-zmozhe-ukraina-ii-zupynyty/>, (accessed 24.08.2026).
- ¹⁶ Ibidem.
- ¹⁷ J. Struck-Feshchenko, Russia Adds More Rassvet Satellites, Attempting to Build Its Own 'Starlink', 2026, <https://www.kyivpost.com/post/80765> (accessed 24.08.2026); Д. Шумлянський, Супутники «Рассвет» досягли вікна стабільного покриття у кілька годин зв'язку над Україною, 2026, <https://militalny.com/uk/news/rassvet-zmozhut-zabezpechyty-rosiyi-zvyazok/>, (accessed 24.08.2026).
- ¹⁸ A. Skujins, From Garpiya drones to a Starlink rival: Europe strikes at Russia's military might, 2026, <https://www.euronews.com/my-europe/2026/07/27/from-garpiya-drones-to-a-starlink-rival-europe-strikes-at>

- russias-military-might, (accessed 24.08.2026).
- 19 The Landlord Lost the Keys: Russia's War Gamechanger in Low Orbit, 2026, <https://southfront.press/the-landlord-lost-the-keys-russias-war-gamechanger-in-low-orbit/>, (accessed 24.08.2026).
 - 20 Ibidem.
 - 21 B. Lindsay, W. MeyerAshley, CraigElizabeth (Liz), K. Lowe, Ashley T. Luong, Expansive New Sanctions Are Imposed on Russia to Address Concerns over Election Interference, Crimea, and Cyber Attacks, 2021, <https://www.venable.com/insights/publications/2021/04/expansive-new-sanctions-are-imposed-on-russia>, (accessed 24.08.2026).
 - 22 16th package of sanctions on Russia's war of aggression against Ukraine: EU lists additional 48 individuals and 35 entities, 2025, <https://www.consilium.europa.eu/en/press/press-releases/2025/02/24/16th-package-of-sanctions-on-russia-s-war-of-aggression-against-ukraine-eu-lists-additional-48-individuals-and-35-entities/>, (accessed 24.08.2026)
 - 23 V. Olari, Romanian channel launders sanctioned Russian content for domestic audiences, 2026, <https://dfirlab.org/2026/03/20/romania-n-channel-launders-sanctioned-russian-content-for-domestic-audiences/>, (accessed 24.08.2026).
 - 24 V. Châtelet and A. Lesplingart, Russia's Pravda network in numbers: Introducing the Pravda Dashboard, 2025, <https://dfirlab.org/2025/04/18/introducing-the-pravda-dashboard/>, (accessed 24.08.2026).
 - 25 V. Châtelet, Exposing Pravda: How pro-Kremlin forces are poisoning AI models and rewriting Wikipedia, 2025, <https://www.atlanticcouncil.org/blog-s/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-and-rewriting-wikipedia/>, (accessed 24.08.2026).
 - 26 Pravda in the pipeline: Early evidence of state-adjacent propaganda in AI training data, 2026, <https://dfirlab.org/2026/04/08/pravda-in-the-pipeline/>, (accessed 24.08.2026).
 - 27 І. Бережанський, У ЦПД пояснили, навіщо Путін знову почав погрожувати ракетою «Сармат», 2026, <https://tsn.ua/ato/u-tspd-poisnylynavishcho-putin-znovu-pochav-pohrozuvaty-raketoiu-sarmat-3081992.html>, (accessed 24.08.2026); А. Кузьмін, «Аналогов нет». Фейкова зброя Російської Федерації, 2022, <https://glavcom.ua/publications/analogov-njet-fejkova-zbroja-rosijskoji-federatsiji-892606.html>, (accessed 24.08.2026).
 - 28 Н. Клочко, Птахи-вбивці та бойові комарі. Росія в ООН видала нову порцію абсурдних заяв, 2022, <https://glavcom.ua/world/world-politics/ptakhi-vbivtsi-ta-bojovi-komari-predstavnik-rosiji-v-on-vidav-novu-portsiju-absurdnikh-zajav-885340.html>, (accessed 24.08.2026).

Bibliography

Books

- HOFFMAN, Franc G. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007, p. 29.

МАГДА, Є., *Гібридна війна: вижити і перемогти*, Харків, 2015.

Online resources

- 16th package of sanctions on Russia's war of aggression against Ukraine: EU lists additional 48 individuals and 35

- entities, 2025, <https://www.consilium.europa.eu/en/press/press-releases/2025/02/24/16th-package-of-sanctions-on-russia-s-war-of-aggression-against-ukraine-eu-lists-additional-48-individuals-and-35-entities/>.
- CHÂTELET, V. and LESPLINGART, A., *Russia's Pravda network in numbers: Introducing the Pravda Dashboard*, 2025, <https://dfirlab.org/2025/04/18/introducing-the-pravda-dashboard/>.
- CHÂTELET, V., *Exposing Pravda: How pro-Kremlin forces are poisoning AI models and rewriting Wikipedia*, 2025, <https://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-and-rewriting-wikipedia/>.
- LINDSAY, B., MEYER, ASHLEY, W., CRAIG, Elizabeth (Liz), Lowe, ASHLEY, K. Lowe, LUONG, T., *Expansive New Sanctions Are Imposed on Russia to Address Concerns over Election Interference, Crimea, and Cyber Attacks*, 2021, <https://www.venable.com/insights/publications/2021/04/expansive-new-sanctions-are-imposed-on-russia>.
- OLARI, V., *Romanian channel launders sanctioned Russian content for domestic audiences*, 2026, <https://dfirlab.org/2026/03/20/romanian-channel-launders-sanctioned-russian-content-for-domestic-audiences/>.
- Pravda in the pipeline: Early evidence of state-adjacent propaganda in AI training data, 2026, <https://dfirlab.org/2026/04/08/pravda-in-the-pipeline/> (accessed 24.08.2026)
- PYNNÖNIEMI, K., JOKELA, M., *Perceptions of hybrid war in Russia: means, targets and objectives identified in the Russian debate*, 2020, <https://www.tandfonline.com/doi/epdf/10.1080/09557571.2020.1787949?needAccess=true>.
- SKUJINS, A., *From Garpiya drones to a Starlink rival: Europe strikes at Russia's military might*, 2026, <https://www.euronews.com/my-europe/2026/07/27/from-garpiya-drones-to-a-starlink-rival-europe-strikes-at-russias-military-might>.
- STRUCK-FESHCHENKO, J., *Russia Adds More Rassvet Satellites, Attempting to Build Its Own 'Starlink'*, 2026, <https://www.kyivpost.com/post/80765>.
- The Landlord Lost the Keys: Russia's War Gamechanger in Low Orbit, 2026, <https://southfront.press/the-landlord-lost-the-keys-russias-war-game-changer-in-low-orbit/>.
- 20 лютого: початок окупації Криму і війни Росії проти України, 2025, <https://crimea-platform.org/news/20l-i-utoho-pochatok-okupatsii-krymu-iviy-ny-rosii-proty-ukrainy/>
- БАЛЮВСЯК, Н., «Шторм-1516» та інші: як Росія створила глобальну екосистему інформаційного впливу, 2026, <https://tyzhden.ua/shtorm-1516-ta-inshi-iak-rosiia-stvoryla-hlobalnu-ekosystemu-informatsijnoho-vplyvu/>.
- БЕРЕЖАНСЬКИЙ, І., У ЦПД пояснили, навіщо Путін знову почав погрожувати ракетою «Сармат», 2026, <https://tsn.ua/ato/u-tspd-poiasn-ly-navishcho-putin-znovu-pochav-pohrozuvaty-raketoiu-sarmat-308199-2.html>.
- Від «Їх там немає» до «Що приховувати?»: як Росія заперечувала, а потім визнала захоплення Криму, 2019, <https://www.radiosvoboda.org/a/krym-putin-rosijski-vijskovi/2979-2-092.html>.
- Кислиця в ООН: Росія вигравіювала на медалі дату початку агресії проти України, 2021, <https://unn.ua/news/>

- kislitsya-v-on-rosiya-vigrav-iyuvala-na-medali-datu-pochatku-agresiyi-p-roti-ukrayini.
- КЛОЧКО, Н., *Птахи-вбивці та бойові комарі. Росія в ООН видала нову порцію абсурдних заяв*, 2022, <https://glavcom.ua/world/world-politics/ptakhi-vbivtsi-ta-bojovi-komari-predstavnik-rosiji-v-onn-vidav-novu-porciju-absurdnikh-zajav-885340.html>.
- КРУПКА, А., *Росія створює альтернативу Starlink: чи зможе Україна її зупинити*, 2026, <https://tyzhden.ua/rosiia-stvoriue-alternatyvu-starlink-chy-zmozhe-ukraina-i-zupynyty/>.
- КУЗЬМІН, А., *«Аналогов нет». Фейкова зброя Російської Федерації*, 2022, <https://glavcom.ua/publications/analohov-njet-fejkova-zbroja-rosijskoji-federatsiji-89260-6.html>.
- МОЛЯР, І., *Це вкрай небезпечно для нас: Грабський про угруповання російських супутників "Рассвет"*, 2026, <https://espreso.tv/viy-na-z-ro-siyeyu-tse-vkray-nebezpechno-dlya-n-as-grabskiy-pro-ugrupovannya-ro-siy-skikh-suputnikov-rassvet>.
- ПИЛИПІВ, І., *Росія втратила Starlink і буде заміню. Що відомо про систему "Рассвет", Економічна правда*, 2026, <https://pravda.com.ua/svit/rosiya-rozvivaye-vlasniy-suputnikoviy-internet-zagroza-dlya-ukrajini-824130/>.
- Російська дезінформація у 2026 році: нові кампанії та інструменти, 2026, <https://www.united-ukraine.org.ua/post/russian-disinformation-in-2026-new-campaigns-and-tools>.
- Російська дезінформація у 2026 році: нові теми та інструменти. Аналітична доповідь, 2026, <https://www.united-ukraine.org.ua/post/russian-disinformation-in-2026-new-topics-and-tools>.
- Росія прискорила будівництво власного аналогу Starlink, 2026, <https://newformat.info/socium/rosiia-pryskoryla-budivnytstvo-vlasnoho-analohu-starlink/>.
- ШУМЛЯНСЬКИЙ, Д., *Супутники «Рассвет» досягли вікна стабільного покриття у кілька годин зв'язку над Україною*, 2026, <https://military.com/uk/news/rassvet-zmozhut-zabezpechity-rosiyi-zvyazok/>.