Daniel Boćkowski

https://orcid.org/0000-0002-0444-6849

University of Białystok

Russian Intoxication Operations and Ways of Building Societal Resilience

Zarys treści: Celem pracy jest opisanie zjawiska operacji intoksykacyjnych prowadzonych przez Federację Rosyjską, na przykładzie Polski, oraz analiza, jak budować odporność społeczną na takie działania, biorąc pod uwagę „zakażanie" AI, zjawisko efektu potwierdzenia oraz przełamywanie kotwic mentalnych.

Outline of content: The aim of the study is to describe the phenomenon of intoxication operations conducted by the Russian Federation, using Poland as a case study, and to analyse how societal resilience to such activities can be built, considering the 'poisoning' of AI, the confirmation bias effect and the process of overcoming mental anchoring.

Słowa kluczowe: operacje intoksykacyjne, dezinformacja jako narzędzie, wojna kognitywna, psyop Federacji Rosyjskiej, odporność

Keywords: intoxication operations, disinformation as a tool, cognitive warfare, Russian Federation PSYOPS, resilience

Introduction

Disinformation has become one of the most frequently used terms in analyses explaining the drivers of change in today's world. Fake news, lies, trolls and cognitive warfare are concepts that describe a broad spectrum of activities aimed at destabilising democratic states internally, undermining trust in them and fostering a constant sense of threat that causes true information to drown in a sea of falsehoods. Public confidence in reliable sources is eroding. Almost all think tanks, analytical platforms and governmental and non-governmental agencies monitoring information networks identify the Russian Federation as one of the most active actors in this field, pointing to the growing importance of information warfare and intoxication in the Kremlin's foreign policy.

Purpose and scope of the work

The present study undertakes a concise comparative analysis of the core elements of intoxication as employed in psychological operations (PSYOPS), and it seeks to identify measures that may prove effective in fostering societal and individual resilience to such influence activities. These procedural frameworks are referred to, among other things, as 'social immunisation', understood as a process of cultivating collective resilience to the phenomenon itself rather than to the associated content, which is of secondary importance. A well-designed intoxication operation can easily be repurposed to pursue new objectives by simply altering the content imprinted into collective consciousness. Attempting to break through the information (filter) bubble reinforced by algorithms is a relatively inefficient strategy. However, it proves more efficient to teach individuals to recognise harmful patterns when encountered, or, during various discussions, to skilfully guide interlocutors to identify gaps in their imprinted 'own' beliefs.

The central research thesis posits that societal resistance to intoxication operations can be cultivated through a combination of profiled education, targeted communication and the identification of recurring patterns in Russian PSYOP campaigns, thereby enabling the development of discipline-specific "disinformation vaccines" based on existing regulatory frameworks (NATO, EU).

The analysis focuses on two selected operations, in which slogans such as 'Volhynia', 'migration threat' and 'not our war' function as mental anchors to construct access paths to memory, thereby maximising the efficacy of intoxication operations.

Research methodology

The study employs analytical and comparative analysis with elements of qualitative research. The research methods used include: a) content analysis (examining selected Russian narratives and media messages), b) comparative analysis (focusing on resilience strategies in Poland) and c) case studies (discussing specific intoxication operations and social reactions). The investigation employs two research techniques: a review of academic sources and expert reports, and a qualitative analysis of media content (Twitter/X, Telegram and news portals). Due to the intended length of the article, not all methods and techniques used are fully reflected in the final text.

Definition of the phenomenon

The phenomenon of 'information intoxication' exploits a state of mind known as information overload (infobesity), a condition in which the volume of incoming data exceeds an individual's cognitive capacity to absorb it, leading to diminished

efficiency in processing, analysing and understanding it, thereby triggering a cascade of errors.[1] When intoxication functions as a tool within psychological operations, this involves a deliberate dissemination of large volumes of diverse information intended to confuse, disorient, or fatigue recipients, ultimately limiting their capacity for critical reasoning and informed decision-making. Jerzy Zalewski draws attention to this phenomenon, identifying information intoxication as "the main element of the information warfare conducted by the Russian Federation".[2]

These activities are further facilitated by the fact that contemporary society can, in many respects, be described as a society *addicted to information*. The dependence on rapidly aggregated images, sounds and short video clips facilitates the covert insertion of mental anchors into memory. Whereas social-media and search-engine algorithms, increasingly coupled with AI, subsequently lock the recipient into an information bubble meticulously engineered by the adversary. Consequently, when these dynamics align with the strategic objectives of the Russian Federation, they constitute operations that form part of a broader strategy to influence public opinion, undermine social trust, foster polarisation and generate destabilisation.

Key differences between disinformation, psychological operations (PSYOPS) and intoxication, taking into account both civilian and military categories:

- Disinformation – the deliberate dissemination of false or partially false information intended to mislead recipients (undermining trust, provoking information chaos and fostering destabilisation; its key features include false, partially false, or true information deliberately 'poisoned' with false elements, the recipient remains unaware of the deception, it can be tailored for a specific target or for the masses and it is now primarily disseminated through social media;[3]
- Psychological operations (PSYOPS) – planned military or civilian operations designed to influence the perception, morale and behaviour of specific groups; their key features include functioning as a destabilising instrument, possessing a precisely defined target and almost always combining information, emotions and cultural context as carriers and mental anchors. The main objective is to support specific military operations, including those

---

[1] The term originated in the 1970s, when writer Alvin Toffler warned about the negative effects of data overload. In his novels, he described society's reaction to rapid technological change. See: E. Rose Jones, 'Information Overload', thedecisionlab.com (2021), https://thedecisionlab.com/reference-guide/psychology/information-overload (accessed 12 Sept. 2025); J. Zieliński, 'Przeciążenie informacyjne we współczesnym procesie edukacyjnym człowieka', *Kultura – Przemiany – Edukacja*, 14–15 (2024), pp. 114–128, https://doi.org/10.15584/kpe.2024.7 (accessed: 12 Sept. 2025).

[2] J. Zalewski, 'Intoksykacja psychologiczno-informacyjna głównym elementem wojny informacyjnej prowadzonej przez Federację Rosyjską', *Studia Bezpieczeństwa Międzynarodowego*, 9, no. 1 (2016), pp. 201–220, https://doi.org/10.37055/sbn/129826 (accessed: 12 Sept. 2025).

[3] E. Surawy Stepney, C. Lally, *Disinformation: Sources, Spread and Impact*, POSTnote Series, no. 719 (25 April 2024), https://researchbriefings.files.parliament.uk/documents/POST-PN-0719/POST-PN-0719.pdf (accessed: 12 Sept. 2025).

conducted below the threshold of war and to influence critical political processes.[4]

- Intoxication – a strategy that deliberately floods target audiences with a surplus of competing narratives in order to overload cognitive processing capacity and thereby facilitate the covert insertion of adversarial data, relies on either the multiplication of conflicting messages or the controlled leakage of 'inside information' – ostensibly credible; its key features include operation through the effect of scale, a high degree of sophistication and information that appears to be source-confirmed and it is often targeted at decision-making elites.[5]

Key features of intoxication operations and illustrative examples

Contemporary intoxication operations are high-cost and scalable, characterised by a very large number of messages designed to exist in the infosphere as an 'amplifier' in the construction of information bubble algorithms. However, they are characterised by repeatability, multi-channel dissemination of desired information, mental anchors (traditional and social media), speed of information delivery, and deliberate repetition aimed at consolidating it, even unconsciously, in recipients' memory. The example that illustrates this modus operandi is the technique known as the 'Firehose of Falsehood', a term coined by RAND analysts to denote the rapid and widespread inundation of audiences with multiple, often contradictory messages, regardless of their veracity.[6] A potential adversary deploys bots, troll farms, 'experts' and influencers to create the impression of social consensus. Importantly, contradictory narratives, half-truths, manipulations and lies can be combined in any proportion within such operations. All of this is intended to lead to the relativisation of true information. Additionally, all available techniques targeting emotions are employed to erode the recipient's ability to assess misinformation rationally, leading to chaos and disorientation of the recipient. The objective is not to persuade the audience of a single narrative, but rather to saturate the information environment with competing narratives, thereby increasing the probability that the authentic message will be 'lost' in the resulting disinformation fog. It may

---

[4] D. Cowan, Ch. Cook, 'What's in a Name? Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change', *Military Review* (6 March 2018), https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/PSYOP/ (accessed: 12 Sept. 2025).

[5] J. Zalewski, *Intoksykacja*.

[6] C. Paul, M. Matthews, 'The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It', *RAND Corporation. Perspectives* (11 July 2016), https://www.rand.org/pubs/perspectives/PE198.html (accessed: 12 Sept. 2025).

be assumed that such operations attempt to normalise mendacity as a legitimate component of public discourse.

In the case of the Russian Federation, such methods have been employed during the Cold War. However, today, due to the development of social networks and information-delivery algorithms, their scale and sophistication are far greater. The primary objective of these operations is to flood the infosphere with diverse messages built on selected mental anchors to induce cognitive overload among recipients.

AI training models increasingly become the target of intoxication operations, and in this scenario, the intoxication does not directly affect the recipient's mind but seeks to 'force' AI algorithms to supply specific disinformation in response to queries. In this way, adversaries can incorporate AI into their narrative as an amplifier and provider of 'trusted' information, which, by virtue of its provenance, may serve to reinforce particular mental anchors, thus constituting a form of 'poisoning' of the model.

In AI models, data, whether true, false, or partially true, is intentionally mixed, which adds an extra layer of protection for conventional intoxication operations. This makes it significantly harder to detect and counter these tactics, especially when the targets are novel and not yet identified. Once specific targets are identified, countering the disinformation campaign and building social resilience become challenging, because the AI-generated message remains permanently 'poisoned', a condition that persists unless supplementary datasets become available for retraining, enabling the removal of deliberately introduced errors. Yet, the efficacy of such countermeasures remains uncertain, especially since the attacking state ensures that the models are exposed to as much fabricated data as possible, embedded in websites built specifically for the purpose of training AI and not for the purpose of deceiving the attacked society. Thus, contemporary operations are combined, and the volume of data generated by these activities grows exponentially.

The effects of such activities, namely, confusion, cognitive fatigue, data overload and erosion of trust, exert an even stronger impact on recipients, who thereby become less vigilant or tend to reject all messages as suspicious. In such circumstances, turning to AI-generated information may subconsciously reinforce narratives favoured by, for example, the Russian Federation.[7] The weakening of societal resilience exposes populations that can no longer distinguish reliable information from manipulation to heightened risks of polarisation, internal conflict and loss of trust in institutions. In conditions of open hybrid conflict and destabilising or diversionary activities, information becomes a basic instrument of warfare, which makes intoxication operations a threat not only to information but also to national security. In its official statements, the Russian Federation openly acknowledges

---

[7] We need also remember that such operations are carried out by other centres under false flags.

that it is effectively at war with NATO, which actively supports Ukraine, thus legitimising, from its perspective, all operations, including kinetic ones, conducted below the threshold of war. All these activities are also intended to influence the societies of European countries and reinforce combined PSYOPS and intoxication operations.

Understanding the mechanisms of intoxication remains essential for formulating protective and defensive strategies, a necessity that extends to the armed forces, state agencies, and civil society. Since intoxication operations proceed continuously, they frequently exploit already established and consolidated access paths and mental anchors. Therefore, defensive measures cannot rely solely on the ex post facto identification and refutation of false information. False data introduced into circulation and embedded in the online environment do not disappear. If the basic principles of quantum physics informed the analysis, this data would remain in a kind of superposition, formally invisible and inaccessible to the user until it is invoked. Only once the attacking side succeeds in introducing and consolidating key words or mental anchors within public consciousness and a potential victim poses a specific query, does the algorithmic mechanism activate: it reaches into the network. It delivers what it considers the most adequate answer. This process occurs at a level analogous to the measurement of a physical system in quantum mechanics.[8] The information that the algorithm retrieves thus indirectly 'decides' the subsequent trajectory of the entire system, and, if the recipient responds positively, that is, by clicking and assimilating the transmitted data, the algorithm's subsequent behaviour becomes contingent upon that initial moment when the (mis)information triggers a form of wave-function collapse.

Data aggregation and transmission determine the recipient's cognitive experience, directly influencing the formation of mental anchors assigned to that particular 'state' of information. Hence, the greater the volume of data compressed into network repositories, the easier it becomes for the adversary to select and 'imprint' the (mis)information of interest onto the recipient's memory. Subsequently, the flood of analogous or similar data leads to cognitive overload, disabling the recipient's ability to verify the message's accuracy. The next stage is enclosure within an information bubble, combined with the confirmation bias that prevents potential recognition of falsehood.[9] The cumulative effect of these processes is both cognitive intoxication of the recipient and reinforcement of the algorithm responsible for retrieving specific data.

---

[8] 'How to Learn Quantum Physics: A Beginner's Guide', www.spinquanta.com (19 Jan. 2025), https://www.spinquanta.com/news-detail/how-to-learn-quantum-physics-a-beginners-guide20250116105706 (accessed: 15 Sept. 2025).

[9] S. Plous, *The Psychology of Judgment and Decision Making* (New York, 1993); see also J. Risen, T. Gilovich, 'Informal Logical Fallacies', in *Critical Thinking in Psychology*, ed. R.J. Sternberg, H.L. Roediger III, D.F. Halpern (New York, 2012), pp. 110–130, https://doi.org/10.1017/CBO9780511804632 (accessed: 15 Sept. 2025).

Table 1. Stages of poisoning with misinformation

Stage I	Stage II	Stage III	Effect	Result
Poisoning with misinformation	Mental anchoring	Locking in an information bubble	Confirmation bias, which blocks recognition of misinformation	Recipient intoxication, the reinforcement of the algorithm responsible for retrieving false data

Consequently, the above stages yield a closed system that is extremely difficult to disable, and when additional 'poisoning' actions, such as impersonating trusted sources or leveraging AI to generate manipulated content, are introduced, the attacking party gains a diverse toolkit for the internal destabilisation of the state and society.

Therefore, the following section examines several selected Russian operations that either exploited existing mental anchors or created new ones, which were subsequently deployed in multi-layered intoxication campaigns.

The most recent operation conducted by the Russian Federation involves activities directly related to the war in Ukraine. A sustained narrative campaign can be observed – a campaign designed to discredit Western institutions, instil domestic scepticism regarding state legitimacy, suppress further assistance to Ukraine and erode confidence in Ukraine's strategic intentions, escalating when necessary into overt hostility towards Ukrainians, Ukraine and their defensive war. This operation has been conducted continuously since 2015, following the annexation of Crimea and the outbreak of the war in Donbas initiated by the Russian Federation. Its objectives included weakening Ukraine's international standing, undermining efforts to challenge Russia's status quo on the peninsula, projecting an image of Russia's unquestionable agency in its pursuit of open territorial revision in Europe and cultivating the belief in its overwhelming military and technological superiority.[10] One of the most significant mental anchors at that time was the slogan of protecting Russians and the supposed right of 'Russian-speaking communities' to self-determination.

Following February 2022, the primary Russian narrative shifted towards the West, with particular focus on Poland. At that point, Russia attempted to exploit a long-standing mental anchor: Volhynia – UPA – atrocities against Poles. Russia has employed these slogans whenever it sought to block emerging forms of Polish-Ukrainian cooperation, deliberately directing this messaging toward far-right circles in Poland.[11] Over time, this narrative became increasingly present in public

---

[10] I often refer to these actions as the 'pufferfish strategy' (*takifugu rubripes*, commonly known as the Japanese puffer). On the eve of the attack on Ukraine, numerous Russian military exercises were intended to reinforce the Russian military's belief in its power and the futility of resistance, and to deter any assistance from European countries.

[11] K. Baraniuk, *Walka informacyjna jako środek realizacji polityki zagranicznej Federacji Rosyjskiej. Przykład trollingu w polskojęzycznej cyberprzestrzeni* (PhD diss.), Uniwersytet Wrocławski,

discourse, leading to a noticeable decline in support for Ukraine, for its defensive war, and for the presence of Ukrainian war refugees in Poland. When comparing Polish society's attitudes toward Ukraine and its citizens in 2022 and 2025, it is clear that this disinformation campaign proved successful for the Russian Federation.[12] It can be said that the long-standing mental anchor, constructed shortly after the Second World War, became the strongest factor reinforcing the confirmation bias. The second mental anchor that the Russian Federation attempted to implant in the Polish information space, 'this is not our war', did not amplify the Russian narrative and remains unusable.[13] The slogan was also introduced in Western Europe with similarly limited effect.

The second intoxication operation is also linked to Russia's attack on Ukraine. Its unifying element was the refugee crisis artificially generated by Belarus and the Russian Federation on the Polish-Belarusian border. The mental anchor required for this operation had emerged in 2015 during the migration crisis that affected the whole of Western Europe. In the Polish media space, due to right-wing politicians, a narrative appeared portraying refugees as a threat to national security.[14] This slogan was used during the election campaign and amplified by social media. During the same period, the Russian Federation conducted numerous destabilising operations in Germany and other Western European countries intended to intensify fears associated with migrants. In Poland, it most likely reinforced anti-refugee messages as part of broader efforts to polarise the society internally. The refugee crisis began in 2020 and resulted in profound polarisation. The first attempt at an intoxication operation involved fabricating and amplifying claims about crimes allegedly committed by Polish soldiers guarding the border against defenceless migrants, alongside the strengthening of anti-migrant slogans aimed at undermining public trust in the state's security institutions.[15] The goal of these

---

([Wrocław], n.d.), https://repozytorium.uni.wroc.pl/Content/132316/PDF/Kamil%20Baraniuk%20doktorat%20pdf%5B5683%5D.pdf (accessed: 12 Sept. 2025); A. Goszczyński, *Dezinformacja i propaganda w polityce historycznej Federacji Rosyjskiej wobec Polski i Ukrainy (na podstawie publikacji w rosyjskich i prorosyjskich portalach internetowych w 2023 r.). Raport*, Przeszłość/Przyszłość. Raport Fundacji im. Janusza Kurtyki Series (Warszawa, 2023), https://fundacjakurtyki.pl/wp-content/uploads/2024/01/Dezinformacja-i-propaganda-w-polityce-historycznej-Federacji-Rosyjskiej-wobec-Polski-i-Ukrainy_RAPORT.pdf (accessed: 16 Sept. 2025).

[12] J. Scovil, *Polacy o potencjalnym zakończeniu wojny w Ukrainie*, CBOS. Komunikat z Badań Series, no. 22 (Warszawa, 2025), https://www.cbos.pl/PL/publikacje/raporty_tekst.php?id=6982 (accessed: 16 Sept. 2025).

[13] 'Zewnętrzne linie narracyjne obecne w polskiej infosferze', *NASK.Magazyn* (5 Nov. 2024), https://www.nask.pl/magazyn/zewnetrzne-linie-narracyjne-obecne-w-polskiej-infosferze (accessed: 16 Sept. 2025).

[14] P. Sadura, 'The Migration crisis as a Strategy of Struggle for Political Power: The Case of Law and Justice', Heinrich Böll Stiftung, Warsaw, Poland (12 Nov. 2021), https://pl.boell.org/en/2021/11/12/kryzys-migracyjny-jako-strategia-zdobywania-wladzy-przypadek-polski (accessed: 12 Sept. 2025).

[15] J. Scovil, *O sytuacji na granicy polsko-białoruskiej*, CBOS. Komunikat z Badań Series, no. 81 (Warszawa, 2024), https://www.cbos.pl/SPISKOM.POL/2024/K_081_24.PDF (accessed: 16 Sept. 2025).

actions was to trigger a crisis on the Polish-Ukrainian border at the moment of Russia's invasion of Ukraine. The Russian Federation sought to employ the previously mentioned Volhynia – UPA mental anchor together with the newer 'migrant threat' anchor to provoke extremely negative reactions among Poles toward the mass influx of Ukrainian war refugees.

Despite thorough preparation, the intoxication operation failed. Russia underestimated an even stronger factor present in Poland: societal support for anyone resisting Russia. More on this topic, including the 'Sluice' Operation, is discussed in an analysis published in *Dzieje Najnowsze* in 2024.[16]

Building societal resilience

In developing elements of societal resilience to intoxication activities and bearing in mind the negative role of a 'deceived' AI, the starting point must be the concept of *resilience* as understood in the context of information security. Referring to the doctrinal framework and drawing on NATO's definition, where *resilience* is defined as "the individual and collective capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions",[17] the objective becomes enhancing the capacity of the state and society to operate effectively in the face of information threats by increasing resistance to overload caused by contradictory or mutually exclusive data and by improving the ability to absorb them. This can be pursued through two pathways. The first pathway is fostering cognitive resilience by enabling recognition of manipulation, disinformation, and propaganda, combined with the cultivation of critical thinking among potential recipients of misinformation. This pathway must additionally be supported by the state through efficient response procedures (fact-checking, strategic communication) and coherence among public institutions responsible for resilience-building. The second pathway involves strengthening natural societal resilience by broadly disseminating examples of intoxication operations and informing recipients about the biological aspects of information reception and aggregation, thus increasing self-awareness. This second pathway, therefore, enters the educational dimension of societal resilience development.

---

[16] See D. Boćkowski, 'Kryzys migracyjny na wschodniej granicy Polski 2015–2022/2024 jako element wielopoziomowej operacji wpływu Federacji Rosyjskiej', *Dzieje Najnowsze*, no. 4 (2024), pp. 213–227, https://doi.org/10.12775/DN.2024.4.10 (accessed: 12 Sept. 2025); Bryjka F., Legucka A., *Russian and Belarusian Disinformation and Propaganda in the Context of the Polish-Belarusian Border Crisis*, PISM Bulletin Series, no. 212 (1908), 9 Dec. ([Warsaw], 2021), https://www.pism.pl/publications/russian-and-belarusian-disinformation-and-propaganda-in-the-context-of-the-polish-belarusian-border-crisis (accessed: 18 Sept. 2025).

[17] 'Resilience, Civil Preparedness and Article 3', www.nato.int (13 Nov. 2024), https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3 (accessed: 18 Sept. 2025).

When intoxication activities succeed, and resilience barriers are breached, it becomes necessary to develop specific 'vaccines' that can rebuild internal, individual resistance. This process primarily relies on overcoming confirmation bias. Such a vaccine should be based on mental anchors developed by psychologists, biologists, linguists and cognitive scientists, designed to prompt individuals trapped within information bubbles to seek out inconsistencies in narratives they perceive as true. Similar vaccines may also be employed to strengthen societal resilience through systemic state education programs, initiatives that activate civil society in the areas of digital resilience and media literacy and support for media outlets that reduce reliance on click-driven content designed to provoke emotional reactions and intensify the hunger for information. What ultimately shields a population from cognitive intoxication is the cultivation of the largest possible repository of 'positive' information, while recognising that 'negative' information exerts a far stronger impact on consciousness, which is one of the natural characteristics of the human brain.

Conclusion

Intoxication constitutes a qualitatively distinct and particularly dangerous tool of information warfare, going beyond classical disinformation. Its essence is not to persuade the recipient of a single version of reality, but to induce deliberate cognitive overload, leading to disorientation, the relativisation of truth, and the erosion of trust in all sources of information. In this sense, intoxication functions as a catalyst for social and political chaos.

The Russian Federation employs intoxication operations in a systematic, long-term, and adaptive manner, combining experience from the Cold War with capabilities enabled by social media, recommendation algorithms, and artificial intelligence tools. The scale, repetitiveness and multi-channel nature of these activities significantly amplify their effectiveness, particularly in democratic societies built on the free flow of information.

A key element of the effectiveness of intoxication operations lies in mental anchors, deeply rooted in collective memory and in the emotions of recipients. Examples such as the slogans 'Volhynia', 'migration threat', or 'protection of Russian speakers' demonstrate that the older and more emotionally and culturally charged an anchor is, the easier it becomes to reactivate and exploit it in order to construct new destabilising narratives.

The analysis of selected cases indicates that the effectiveness of Russian intoxication operations is variable and dependent on the social context and on competing mental anchors. The operation employing the Volhynia narrative against Poland proved effective in the long term, whereas the attempt to link the migration crisis with the influx of war refugees from Ukraine failed due to the presence of a stronger counter-anchor – Poland's historical and emotional opposition to Russia.

The development and deployment of artificial intelligence within the infosphere significantly exacerbates the problem of intoxication, as it shifts its focus from direct influence on the recipient to the 'poisoning' of algorithms and language models. As a result, AI can become not only a tool of information warfare but also a force multiplier, lending false or manipulated content an appearance of objectivity and credibility.

Building societal resilience cannot rely solely on fact-checking and debunking false information, as data introduced into the information space does not disappear, and algorithms can continue to reactivate it. Effective defence requires moving away from a reactive model of responding to content toward proactively strengthening recipients' cognitive competencies.

The most promising approach to countering intoxication operations is the concept of 'social immunisation', which combines targeted media education, directed strategic communication and the systematic use of NATO and EU resilience frameworks. Teaching people to recognise patterns of manipulation and underlying psychological mechanisms proves more effective than combating individual narratives.

A particularly important role is to overcome confirmation bias, which traps individuals and social groups in information bubbles. Developing 'disinformation vaccines' grounded in psychological, cognitive and linguistic knowledge may help rebuild resilience at both the individual and collective levels.

Ultimately, intoxication operations should be understood not merely as an information threat but as a component of national security, capable of destabilising a state without the use of kinetic force. Understanding their mechanisms and implementing multi-layered resilience strategies has become one of the key conditions for the functioning of democratic states in an environment of permanent hybrid conflict.

Abstract

The article examines information intoxication as an advanced instrument of contemporary psychological operations, primarily employed by the Russian Federation within information warfare and hybrid conflict. The author distinguishes intoxication from classical disinformation and PSYOPS, emphasising its key feature: deliberate cognitive overload aimed at disorientation, the relativisation of truth, and the erosion of social trust. The study is based on content analysis, comparative analysis and case studies of selected Russian influence operations, with particular attention to narratives related to the war in Ukraine, including 'Volhynia', 'migration threat', and 'this is not our war'. The article also addresses the growing role of social media algorithms and artificial intelligence as force multipliers of intoxication, including the problem of AI model poisoning. It argues that effective countermeasures cannot rely solely on reactive fact-checking, as manipulated information remains present in the information environment. Instead, the author advocates for building cognitive and societal resilience through targeted education, strategic communication and the development of so-called 'disinformation vaccines' grounded in existing NATO and EU resilience frameworks.

References

Baraniuk K., *Walka informacyjna jako środek realizacji polityki zagranicznej Federacji Rosyjskiej. Przykład trollingu w polskojęzycznej cyberprzestrzeni* (PhD diss.), Uniwersytet Wrocławski, ([Wrocław], n.d.), https://repozytorium.uni.wroc.pl/Content/132316/PDF/Kamil%20Baraniuk%20doktorat%20pdf%5B5683%5D.pdf.

Boćkowski D., 'Kryzys migracyjny na wschodniej granicy Polski 2015–2022/2024 jako element wielopoziomowej operacji wpływu Federacji Rosyjskiej', *Dzieje Najnowsze*, no. 4 (2024), pp. 213–227, https://doi.org/10.12775/DN.2024.4.10.

Bryjka F., Legucka A., *Russian and Belarusian Disinformation and Propaganda in the Context of the Polish-Belarusian Border Crisis*, PISM Bulletin Series, no. 212 (1908), 9 Dec. ([Warsaw], 2021), https://www.pism.pl/publications/russian-and-belarusian-disinformation-and-propaganda-in-the-context-of-the-polish-belarusian-border-crisis.

Cowan D., Cook Ch., 'What's in a Name? Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change', *Military Review* (6 March 2018), https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/PSYOP/.

Goszczyński A., *Dezinformacja i propaganda w polityce historycznej Federacji Rosyjskiej wobec Polski i Ukrainy (na podstawie publikacji w rosyjskich i prorosyjskich portalach internetowych w 2023 r.). Raport*, Przeszłość/Przyszłość. Raport Fundacji im. Janusza Kurtyki Series (Warszawa, 2023), https://fundacjakurtyki.pl/wp-content/uploads/2024/01/Dezinformacja-i-propaganda-w-polityce-historycznej-Federacji-Rosyjskiej-wobec-Polski-i-Ukrainy_RAPORT.pdf.

'How to Learn Quantum Physics: A Beginner's Guide', www.spinquanta.com (19 Jan. 2025), https://www.spinquanta.com/news-detail/how-to-learn-quantum-physics-a-beginners-guide20250116105706.

Paul C., Matthews M., 'The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It', *RAND Corporation. Perspectives* (11 July 2016), https://www.rand.org/pubs/perspectives/PE198.html.

Plous S., *The Psychology of Judgment and Decision Making* (New York, 1993).

'Resilience, Civil Preparedness and Article 3', www.nato.int (13 Nov. 2024), https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.

Risen J., Gilovich T., 'Informal Logical Fallacies', in *Critical Thinking in Psychology*, ed. R.J. Sternberg, H.L. Roediger III, D.F. Halpern (New York, 2012), pp. 110–130, https://doi.org/10.1017/CBO9780511804632.

Rose Jones E., 'Information Overload', www.thedecisionlab.com (2021), https://thedecisionlab.com/reference-guide/psychology/information-overload.

Sadura P., 'The Migration crisis as a Strategy of Struggle for Political Power: The Case of Law and Justice', Heinrich Böll Stiftung, Warsaw, Poland (12 Nov. 2021), https://pl.boell.org/en/2021/11/12/kryzys-migracyjny-jako-strategia-zdobywania-wladzy-przypadek-polski.

Scovil J., *O sytuacji na granicy polsko-białoruskiej*, CBOS. Komunikat z Badań Series, no. 81 (Warszawa, 2024), https://www.cbos.pl/SPISKOM.POL/2024/K_081_24.PDF.

Scovil J., *Polacy o potencjalnym zakończeniu wojny w Ukrainie*, CBOS. Komunikat z Badań Series, no. 22 (Warszawa, 2025), https://www.cbos.pl/PL/publikacje/raporty_tekst.php?id=6982.

Surawy Stepney E., Lally C., *Disinformation: Sources, Spread and Impact*, POSTnote Series, no. 719 (25 April 2024), https://researchbriefings.files.parliament.uk/documents/POST-PN-0719/POST-PN-0719.pdf.

Zalewski J., 'Intoksykacja psychologiczno-informacyjna głównym elementem wojny informacyjnej prowadzonej przez Federację Rosyjską', *Studia Bezpieczeństwa Międzynarodowego*, 9, no. 1 (2016), pp. 201–220, https://doi.org/10.37055/sbn/129826.

'Zewnętrzne linie narracyjne obecne w polskiej infosferze', *NASK.Magazyn* (5 Nov. 2024), https://www.nask.pl/magazyn/zewnetrzne-linie-narracyjne-obecne-w-polskiej-infosferze.

Zieliński J., 'Przeciążenie informacyjne we współczesnym procesie edukacyjnym człowieka', *Kultura – Przemiany – Edukacja*, 14–15 (2024), pp. 114–128, https://doi.org/10.15584/kpe.2024.7.

Daniel Boćkowski – PhD hab., Professor of the University of Białystok, Head of the Laboratory of International Security at the Faculty of International Relations, University of Białystok; employee of the Tadeusz Manteuffel Institute of History, Polish Academy of Sciences. Editor-in-chief of *Studia z Dziejów Rosji i Europy Środkowo-Wschodniej* (Studies into the History of Russia and Central-Eastern Europe). Deputy editor-in-chief of *Dzieje Najnowsze* (Recent History). Researcher of Polish-Soviet relations during World War II, contemporary Russia and threats to international security. Analyst and commentator of international politics in both social and traditional media.
(daniel.bockowski@gmail.com)