Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 221–238

ISSN 2543-6961
e-ISSN 2720-3093
LICENCJA: CC BY-NC

Juliusz Sikorski
ORCID: 0000-0002-0579-0158-0002-0579-0158
The Jacob of Paradies University in Gorzów Wielkopolski

Proxy Sources in Cognitive Warfare: The Hidden Architecture of Russian Influence Operations in Central Europe

Źródła pośredniczące w wojnie kognitywnej: ukryta architektura rosyjskich operacji wpływu w Europie Środkowej

Abstract
The article analyzes the role of proxy sources – indirect, ostensibly independent sources and conduits of content – as key components of Russian influence operations in Central Europe conducted within the logic of cognitive warfare. Drawing on reports by NATO StratCom COE, Cardiff University, and the ICCT, as well as documented actions by regulators including the European Union, it reconstructs the mechanics of information laundering, delineates a typology and chains of content flow (placement → layering → integration), and presents case studies (Ghostwriter, NewsFront) alongside an analysis of environmental conditions in Poland and the broader region. The conclusions propose indicators for identifying "proxies" and offer policy and institutional recommendations (prebunking, distribution-network audits, intermediary accountability). The article situates proxy sources within the broader architecture of Russian cognitive warfare, which aims to shape not only what audiences think, but how they think and make decisions. The findings are evidence-informed and derive from a qualitative review of secondary data.

Keywords: cognitive warfare, proxy sources, information laundering, disinformation, propaganda, NewsFront, Ghostwriter, Central Europe, Poland, NATO StratCom

Abstrakt
Artykuł analizuje rolę proxy sources, pośrednich, pozornie niezależnych źródeł i nośników treści, jako kluczowych komponentów rosyjskich operacji wpływu w Europie Środkowej realizowanych w logice walki kognitywnej. W oparciu o raporty NATO StratCom COE, Cardiff University, ICCT oraz udokumentowane działania regulatorów, w tym Unii Europejskiej, dokonano w nim rekonstrukcji mechaniki prania informacji (information laundering), opisano typologię i łańcuchy przepływu treści (lokowanie → warstwowanie → integracja), a także przedstawiono studia przypadków (Ghostwriter, NewsFront) oraz środowiskowe uwarunkowania Polski i regionu. We wnioskach przedstawiono wskaźniki identyfikacji „proxy" oraz rekomendacje polityczne i instytucjonalne (prebunking, audyt sieci dystrybucji, odpowiedzialność pośredników). Artykuł lokuje zjawisko proxy sources w szerszej architekturze rosyjskiej wojny kognitywnej, której celem jest kształtowanie nie tylko tego, co myślą odbiorcy, lecz jak myślą i podejmują decyzje. Ustalenia mają charakter evidence-informed i wynikają z przeglądu jakościowego danych zastanych.

Słowa kluczowe: wojna kognitywna, proxy sources, pranie informacji (information laundering), dezinformacja, propaganda, NewsFront, Ghostwriter, Europa Środkowa, Polska, NATO StratCom

1. Introduction: from propaganda and disinformation to cognitive warfare

Contemporary Russian information influence targeting Central Europe has evolved from classic propagandistic and disinformation techniques toward practices that the military and scholarly literature designate as cognitive warfare. These activities are designed to interfere with the cognitive processes of individuals and collectives, with entrenched interpretive schemas, and with decision-making mechanisms.[1] The literature emphasizes that cognitive warfare "strikes at trust as the social binder" and precedes or accompanies the kinetic phase, preparing the adversary's decision-making environment. In the NATO Review's analytical framing, the battlespace in this type of confrontation is the human mind, and the objective is not only to modify what audiences think, but also how they think and act.[2]

In this context, proxy sources constitute the covert supporting structures of propaganda-disinformation operations. They appear as ostensibly local media outlets, think tanks, blogs, news agencies, and not infrequently as private profiles and micro-influencers. Through overlapping layers of intermediation, they conceal the provenance of the message and lower audiences' threshold of skepticism. They render narratives more concrete by locally anchoring them, while simultaneously serving as content suppliers for channels regarded as at least relatively more credible (mainstream media, political actors, the commentariat).[3] Within such structures, the mechanism known as information laundering is most fully realized.[4]

---

[1] See: F. du Cluzel, *Cognitive Warfare*, Voltairenet, 22 January 2021, pp. 26-27, https://www.voltairenet.org/IMG/pdf/20210122_cognitive_warfare.pdf?utm_source=chatgpt.com [date of access: 29.08. 2025]; Ch. Deppe, G. S. Schaal, *Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept*, "Frontiers in Big Data" 2024, vol. 7, article 1452129, pp. 1-2 https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full [date of access: 29.08.2025]..

[2] K. Cao, S. Glaister, A. Pena, D. Rhee, W. Rong, A. Rovalino, S. Bishop, R. Khanna, J. Singh Saini, *Countering Cognitive Warfare: Awareness and Resilience*, "NATO Review" 20 May 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [date of access: 29.08. 2025].

[3] U.S. Department of State, Global Engagement Center (GEC), *Pillars of Russia's Disinformation and Propaganda Ecosystem,* https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf [date of access: 31.08. 2025]; J. Sikorski, *Źródła pośredniczące (proxy sources) w komunikacji politycznej jako narzędzie walki informacyjnej* [Proxy sources in political communication as a tool of information warfare], [in:] *Komunikowanie polityczne i publiczne w nowych mediach: wybrane przykłady* [Political and Public Communication in New Media: Selected Examples], eds. A. Grzechynka, K. Szmyd, Kraków 2025, pp. 166-187; idem, *Online analytics portal as an information warfare tool of the Russian Federation and its impact after 24 February 2022: case study: RuBaltic.ru*., "Sõjateadlane (Estonian Journal of Military Studies)" 2023, vol. 23, pp. 188-190.

[4] ADMM Cybersecurity & Information CoE (ACICE), *Update on the Information Domain – Information Laundering (Issue 05/24), May 2024*, pp. 1-4, https://www.acice-asean.org/files/may_24_info.pdf [date of access: 29.08. 2025]..

2. Methodology

The aim of this article is to determine the role and operating mechanics of proxy sources – intermediary, ostensibly independent content carriers – within Russian influence operations in Central Europe in the logic of cognitive warfare; to present their typology and the sequencing of narrative flows; to specify indicators for their identification; and to formulate policy-institutional recommendations, with particular emphasis on Poland and its broader Central European environment (in particular the Baltic and Visegrad states).

The study is situated within Critical Security Studies (a constructivist-post-positivist variant with poststructuralist inspirations), which foregrounds the constitutive role of language and discourse in constructing "security problems" and in reproducing or contesting power relations. In this sense, the article draws on the conceptual vocabulary developed by Peoples and Vaughan-Williams and other CSS scholars, treating security not as a fixed condition but as an effect of practices of (in) securitization and meaning-making. At the same time, it engages with the emerging literature on information/technology and warfare that conceptualizes contemporary conflicts as taking place in hybrid, techno-communicative environments shaped by algorithmization, platform logics, and dataveillance practices. By bringing these two strands together, the article adopts a critical perspective on the infrastructural conditions that allow cognitive influence and symbolic violence to be "scaled" through intermediary sources rather than focusing solely on overt propaganda outlets.

The novelty of the approach is threefold. First, it proposes to treat proxy sources as *structural* components of Russian cognitive warfare rather than as merely marginal or auxiliary channels. Second, it links the concept of information laundering to a concrete taxonomy of intermediaries and to empirically documented case studies (Ghostwriter, NewsFront), thus moving beyond purely conceptual treatments. Third, it integrates an analysis of the regional techno-regulatory environment (including DNS-level interventions and sanctions) with a methodology-oriented discussion of how indicators of proxy activity can be operationalized in practice. Taken together, these elements position the article at the intersection of Critical Security Studies, disinformation research, and the emerging debate on cognitive warfare.[5]

The article poses three research questions:

RQ1. What role do proxy sources play in the process of "information laundering," and to what extent do they facilitate the "legalization" of content within mainstream messaging in Central and Eastern Europe?

[5] C. Peoples, N. Vaughan-Williams, *Critical Security Studies: An Introduction – 3rd edition*, Abingdon–New York 2021, pp. 6, 104, 182-183, 197-198.

RQ2. Which indicators best distinguish proxy sources from ordinary content replicators?

RQ3. Under what linguistic–institutional conditions are proxy sources most effective in Poland and the broader Central European region (in particular the Baltic and Visegrad states)?

These questions form an integrated research design. RQ1 focuses on the *functions* of proxies within narrative flows; RQ2 operationalizes this perspective into observable *indicators* that allow proxies to be distinguished from ordinary content aggregators; and RQ3 links both layers to the *contextual conditions* that either facilitate or constrain the effectiveness of proxy sources in Poland and its regional environment. Together, they structure the subsequent empirical sections of the article (architecture of the ecosystem, case studies, regional frameworks, and methodological implications).

On this basis, the following three hypotheses are formulated:

H1. The presence of proxy sources increases the likelihood that a narrative will progress through the sequence placement → layering → integration and enter the mainstream.

H2. Persistent "link bridges"[6] to recognizable hubs, close temporal coincidences, and multilingual replication are key markers of proxy sources.

H3. The effectiveness of proxy sources increases when local linguistic intermediaries are present and verification/response mechanisms within the media ecosystem are weak.

The hypotheses correspond directly to the research questions: H1 mirrors RQ1 by specifying the expected effect of proxies on narrative progression; H2 translates RQ2 into a testable set of diagnostic cues; and H3 provides an empirically oriented answer to RQ3 concerning the enabling conditions of proxy effectiveness. Although a short article format imposes limits on the level of disaggregation, keeping this 3+3 structure makes it possible to maintain an analytically clear distinction between mechanisms (H1), markers (H2), and contextual conditions (H3), while still treating them as parts of a single, coherent research design.

[6] Link bridges are auxiliary, typically low-quality websites created solely to redirect traffic to a target site. This is a so-called black-hat SEO technique, contrary to Google's guidelines, and subject to penalties such as ranking demotion or even removal from the index. Google Search Central, *Spam policies for Google web search*, "Google for Developers" 10 June 2025, https://developers.google.com/search/docs/essentials/spam-policies [date of access: 30.09. 2025]; B. White, *An update on doorway pages*, "Google Search Central Blog" 16 March 2015, https://developers.google.com/search/blog/2015/03/an-update-on-doorway-pages [date of access: 30.09.2025]; Google Support, *Manual actions report,* "Search Console Help" [n.d.], https://support.google.com/webmasters/answer/9044175 [date of access: 30.09.2025]; Google Search Central, *Link best practices for Google*, "Google for Developers" 4 Feb. 2025, https://developers.google.com/search/docs/crawling-indexing/links-crawlable [date of access: 30.09.2025].

Verification of the hypotheses and answers to the research questions were achieved through a qualitative review of the relevant literature and documented case studies. Methodological triangulation – combining cross-linguistic comparisons, reconstruction of citation and link chains, and narrative frame analysis – was used to enhance the reliability of the findings and to ensure that the proposed indicators are robust across different sources and sub-regions of Central Europe.

3. "Proxy sources" and information laundering: definitions, mechanics, indicators

In the NATO StratCom COE's framing, information laundering denotes a process whereby false or misleading content is systematically introduced into circulation via a network of intermediaries so as to obscure the provenance of the message and lend it an appearance of credibility.[7] In turn, at a meeting of ministers responsible for cybersecurity and information from Association of Southeast Asian Nations (ASEAN) member states, it was noted that initiation of this process most often occurs in closed environments (forums, niche channels), from which – using multiple coordinated accounts and platforms – the message gradually permeates mainstream media communications and, through selective fact-picking, contextual manipulation, and the instrumental use of statements by political actors, becomes commingled with credible news until it is fully integrated into the information ecosystem.[8]

In the scholarly literature, the sequence of information laundering comprises three stages:

1. Placement – the initial insertion of content into the public sphere (e.g., on a quasi-portal or blog),
2. Layering – cascading repetitions across related channels, often with references to statements by politicians or to "alternative" media; and
3. Integration – uptake by mainstream media or entry into official debates, which confers a distinctive "quality stamp."[9]

As current findings indicate, these phases may overlap, and the "legalization" of content can result both from an intentional plan and from the opportunistic dynamics of platforms.[10]

---

[7] NATO Strategic Communications Centre of Excellence (NATO StratCom COE), *Information Laundering in Germany*, p. 4, https://stratcomcoe.org/publications/information-laundering-in-germany/23 [date of access: 31.08. 2025].

[8] Ibidem; ACICE, *Update on the Information Domain…*, op. cit., pp. 1-4.

[9] Ibidem.

[10] RESET: Digital for Good, *The Ghostwriter Campaign. A Multi-Vector Information Operation: Attempts to Control Its Influence & the Limitations of Current Countermeasures*, London 2023, pp. 20-22, https://www.reset.tech/publications/the-ghostwriter-campaign-report/ [date of access: 31.08. 2025].

In these processes, proxy sources play a distinctive role, betraying their function through recurrent "link bridges" to a narrow set of hubs (including Sputnik/RT, NewsFront, and the Strategic Culture Foundation), synchronization of publications at short temporal intervals, formulaic multilingual translations, and regular "reciprocal citations" among the same entities (so-called legitimization loops.)[11]

4. The Architecture of the Russian Information Ecosystem and the Role of "Proxies"

International analyses conducted by NATO, the Global Engagement Center (GEC), and the International Centre for Counter-Terrorism (ICCT) consistently indicate that Russian information operations function within an ecosystem that links official state channels with an extensive network of "shell" institutions and intermediaries. The multiplicity of facades plays a crucial role here – ranging from entities masquerading as think tanks, through quasi-news agencies, to simple blogs. The dense web of their covert and ambiguous connections disperses responsibility and complicates the attribution of message sources.[12] From the perspective of cognitive warfare, this mechanism increases the likelihood of reaching diverse audience segments (including experts, military personnel, and activists), while, through "local" intermediaries, it helps to overcome cultural and linguistic barriers.[13]

A variety of entities can be classified as proxy sources. These include quasi-news agencies and "shell" think tanks. Examples of such entities are NewsFront, a quasi-news agency based in the occupied Crimea, and the Strategic Culture Foundation (SCF), a supposedly independent platform for global analysis whose involvement and connections (including with the Foreign Intelligence Service [SVR]) have been identified in both European and U.S. sanction documents.[14]

---

[11] NATO StratCom COE, *Russia's Footprint in the Nordic-Baltic Information Environment: Report 2016/2017*, project director: E. Lange-Ionatamišvili; research team: I. Bērziņa, M. Cepurītis, D. Kaljula, I. Juurvee, Riga 2018, pp. 54-55, 76-77; J. Gallacher, M. Heerdink, *Measuring the effect of Russian Internet Research Agency information operations in online conversations*, "Defence Strategic Communications" 2019, vol. 6, pp. 155-198; T. P. Gerber, J. Zavisca, *Does Russian Propaganda Work?* "The Washington Quarterly" 2016, 39(2), pp. 79-98.

[12] Ch. Deppe, G. S. Schaal, *Cognitive warfare: a conceptual analysis…*, op. cit., pp. 1-3.

[13] F. du Cluzel, *Cognitive warfare…*, op. cit., p. 7; Ch. Deppe, G. S. Schaal, *Cognitive warfare…*, op. cit., pp. 5-8.

[14] Council of the European Union (CEU), *Council Implementing Regulation (EU) 2022/260 of 23 February 2022 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*, "Official Journal of the European Union" 23 Feb. 2022, L 42 I/11; United States. Department of the Treasury. Office of Foreign Assets Control, *Notice of OFAC Sanctions Actions*, Federal Register 20 Apr. 2021, vol. 86, no. 74, p. 20598, 20600-20601 (FR Doc. 2021–08087), https://www.govinfo.gov/content/pkg/FR-2021-04-20/pdf/2021-08087.pdf [date of access:]; M. Leitenberg, *Russian disinformation related to biological weapons, 1998–2021*, annex to: M. Leitenberg, *False allegations of biological-weapons from Putin's Russia*, "The Nonproliferation Review" 2020, vol. 27, nr 4-6, p. 77; supplemental material (appendix),. [do czego appendix?]

The selection of examples used in this article follows a purposive logic. Entities such as NewsFront, the Strategic Culture Foundation, and related "shell" outlets have been repeatedly identified in high-quality analytical reports by NATO StratCom COE, the U.S. State Department's Global Engagement Center, and the International Centre for Counter-Terrorism as central hubs in the Russian disinformation and propaganda ecosystem. They appear not only as content producers but also as organizers of distribution chains that systematically rely on intermediary platforms and local amplifiers. Focusing on these actors makes it possible to trace relatively well-documented chains of content flow – from overt state-linked nodes to ostensibly independent intermediaries – and to illustrate how proxies operate at the intersection of official messaging, social media operations, and cyber-enabled techniques.

These also include intermediaries embedded within the target linguistic environment, as multilingualism is a prerequisite for effectively reaching intended audiences. For instance, NewsFront distributes content in multiple languages, combining a consistent core narrative with localized elements (e.g., anti-immigration slogans in messages aimed at German-speaking audiences, or anti-elitist themes in the English-language version). This mechanism is designed to reinforce the impression of "native media," which are more likely to be cited by politicians and journalists. Their role also involves the multiplication of narratives and the introduction of such narratives into public discourse.[15]

5. Case Studies: The Role of "Proxies" in Credibilizing Narratives

It appears that one of the best-documented examples of the use of proxy sources in disinformation and propaganda campaigns is Operation "Ghostwriter", reconstructed in a 2023 report by Cardiff University. The study revealed the multi-vector nature of the operation, which combined hacking techniques (such as defacement and account takeovers), impersonation of public officials, and the publication of fabricated "articles" on quasi-news portals and blogs that were subsequently systematically amplified. It was established that the campaign's activity dates back to at least 2016, with its initial area of focus being NATO's presence in the Baltic states. Around 2019/2020, the operation's vector expanded to include Poland.

In this context, a significant role was played by the right-wing portal "Niezależny Dziennik Polityczny" (NDP), known for its pro-Kremlin sympathies. The fabricated stories often revolved around recurring narrative frames: questioning the reliability and professionalism of NATO troops deployed in the region, suggesting

[15] See: NATO StratCom COE, *Information Laundering in Germany*, op. cit.; NATO StratCom COE, *Russia's footprint in the Nordic-Baltic information environment…*, op. cit., pp. 6, 32-46, 54, 57, 59, 69, 75-78.

internal fractures within the Alliance, and portraying Polish authorities as subservient to Washington. In several cases documented by investigative outlets and official communications, forged letters or alleged "leaks" were published on quasi-portals, then quickly republished by a network of small websites and social media profiles, which lent them an appearance of independent corroboration. An analysis of the distribution of content published on NDP indicated that dissemination occurred primarily through a network of interconnected social media accounts, especially on Facebook.[16]

The mechanism of dissemination operated as follows: after the publication of fabricated materials on institutional websites,[17] hyperlinks to the alleged "articles" were massively propagated – among others through portals such as lewy.pl, prawy.pl, and podlasie24.pl – which allowed them to achieve significant reach and engagement, while being simultaneously replicated on external platforms (e.g., The Duran, Verity Weekly).[18] A recurrent motif in these texts was the suggestion that the presence of Allied troops undermined local security or that alleged misconduct by soldiers was being deliberately covered up by authorities. Another notable feature was the persistence of some links on Twitter even after the original posts had been removed. Despite the later deletion of NDP accounts on certain platforms, traces of distribution and video materials remained accessible, confirming the durability of the informational contamination effect. Polish intelligence services publicly pointed to the connections between NDP and Russian intelligence activities, emphasizing the risks associated with the continued circulation of such content.[19]

[16] RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 2-4, 6, 9-10, 24.

[17] On April 22, 2020, a cyberattack targeted the website of the War Studies University (Akademia Sztuki Wojennej), during which a forged letter was published, allegedly authored by the commandant, Gen. Ryszard Parafianowicz, calling on Polish soldiers to "rebel" against the "American occupying forces." Subsequently, spoofed emails (impersonating, among others, a former Civic Platform MP and an American journalist) were sent to NATO institutions and Polish government agencies, containing links to the fabricated document. The material was replicated in English on the The Duran website and as "news" on Polish portals lewy.pl, prawy.pl, and podlasie24.pl (which later claimed to have been hacked). The message was further amplified by accounts linked to NDP. The War Studies University warned about the breach the same day on Twitter, and analyses by intelligence services and fact-checkers were published the following day. See: Rzecznik Ministra Koordynatora Służb Specjalnych [Spokesperson for the Minister Coordinator of Special Services], *Atak dezinformacyjny na Polskę [PL/EN]*. Gov.pl – Służby specjalne [*Disinformation attack on Poland* [PL/EN]. Gov.pl – Special Services], April 23, 2020, https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske [date of access: 30.09.2025).

[18] A. Gielewska, *Russia-related accounts and a cyberattack in Poland*, https://vsquare.org/russia-related-accounts-and-a-cyberattack-in-poland/ [date of access: 30.09.2025]; Digital Forensic Research Lab (DFRLab), *Cyber-enabled disinformation campaign targeted U.S.-Poland alliance,* https://dfrlab.org/2020/06/24/cyber-enabled-disinformation-campaign-targeted-u-s-poland-alliance/ [date of access: 30.09. 2025).

[19] RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 6-7; Pełnomocnik Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP [Government Plenipotentiary for the Security of the Information Space of the Republic of Poland], *Rosyjska sieć kłamstw [Russia's web of lies]*, czy to jest źródło internetowe? 2023, pp. 16-17; K. Kuśmirek, *Działania informacyjne Federacji Rosyjskiej w 2023 roku [Information activities of the Russian Federation in 2023]*, "Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30, pp. 90, 347.

A second representative example of the use of proxies is NewsFront, which serves both as a distribution hub and as a kind of narrative "framework." In European Union documents, NewsFront is identified not only as a media outlet but also as an organizer of content flows, directly linked to undermining Ukraine's territorial integrity and destabilizing the region. Operationally, it functions as a "wholesaler" of ready-made narratives, easily adaptable for local "packaging" and distribution. Typical storylines include portraying the EU as being in permanent crisis, questioning the legitimacy of sanctions against Russia, or depicting Ukraine and NATO as aggressive actors responsible for escalation. Once supplied by central "hubs" (such as NewsFront), the introduction of these narratives into national information spaces is carried out by smaller proxies – niche portals, blogs, and social media channels – that increase the likelihood of the messages infiltrating mainstream discourse.[20]

6. "Proxy Sources": Taxonomy, Patterns, Tactics

"Proxy sources" are communication channels formally operating outside state structures, which integrate official messaging, state media, social media operations, and the cyber component, multiplying narratives and giving them an appearance of grassroots authenticity[21]. Based on the Global Engagement Center (U.S. Department of State) framework regarding the pillars of Russian propaganda and disinformation, at least four types of such intermediaries can be distinguished:

1. Semi-official periodicals with an academic façade (e.g., Strategic Culture Foundation, New Eastern Outlook), which serve to legitimize state narratives,
2. Ideologically driven quasi–think tanks (e.g., Katehon, Geopolitica.ru), providing meta-narratives and interpretative frameworks,
3. External amplifiers with a "Western face" (e.g., Global Research), which "launder" the message through cross-publications; and
4. Operational content distributors (e.g., NewsFront, SouthFront), conducting rapid diffusion campaigns.[22]

This perspective is reinforced by the European Union's sanctions framework, which identifies not only the "faces of propaganda" (including Margarita Simonyan, Maria Zakharova, Vladimir Solovyov), but also the operators (e.g., Konstantin Knyrik/NewsFront), online executors (such as the Internet Research Agency), and financial enablers (Bank Rossii, PSB, VEB.RF).[23]

[20] Ibidem, p. 6; CEU, *Council Implementing Regulation (EU) 2022/260*…, op. cit., pp. 8-9.
[21] GEC, *Pillars of Russia's Disinformation and Propaganda Ecosystem*..., op. cit., pp. 7, 11-13.
[22] Ibidem, pp. 14-60.
[23] CEU, *Council Implementing Regulation (EU) 2022/260 of 23 February 2022*…, op. cit., L 42 I, L 42 I/10–L 42 I/14.

In turn, an analysis of the mechanics by which proxy sources operate makes it possible to identify four recurring operational patterns:

1. Building interlingual bridges: the same thesis is rapidly translated and distributed in successive language versions (e.g., EN→DE→PL), with each iteration accompanied by a subtle shift of emphasis (for instance, moving from a focus on "health security" toward "individual freedom" or from "sanctions" toward "economic self-harm"). NATO StratCom COE's studies of information laundering in Germany and the Nordic-Baltic region repeatedly documented identical or near-identical articles appearing across multiple language versions within short intervals, often citing each other as "independent" sources.
2. An amalgam of facts and opinions: combining genuine quotations with an overlaid interpretation, often through misappropriation or the use of misleading language, repeatedly documented in the recommendations of the ADMM Cybersecurity & Information Centre of Excellence (ACICE). In this pattern, seemingly neutral factual statements (e.g., about troop movements or parliamentary debates) are embedded in a narrative frame that suggests hidden motives, conspiracies, or imminent threats, without making explicit factual claims that could be easily disproven.[24]
3. Cyclical activation of "boosters": coordinated, short-term publication of convergent content across several affiliated portals and Telegram/Facebook channels generates a reach impulse (burst) and artifacts of "perceptual consensus." The Ghostwriter campaign provides concrete examples: shortly after the appearance of a forged letter or statement on a quasi-portal, a wave of small sites and social media accounts would circulate similar headlines or commentaries, creating the impression that "everyone is talking about it," even though the content originated from a single operation.
4. "Recycling" scandals: returning to previously fabricated or debunked stories (e.g., the "Lisa 2.0" case in Germany) in new political–media contexts reactivates emotions and keeps the narratives in circulation. Here, minor modifications (such as changing the location, alleged victim, or institutional actor) give the impression of a "new" case, while the underlying storyline – for example, that authorities allegedly conceal crimes or that migrants are systematically protected from accountability – remains stable. Such recycling has been observed both in the German-language and Central European information spaces.[25]

[24] ACICE stands for ADMM Cybersecurity & Information Centre of Excellence, a regional cooperation center operating at the ASEAN Defense Ministers' Meeting. Established in June 2021, its mission is to support information exchange and build defense capabilities in ASEAN against cyberattacks and disinformation. ASEAN, *About ADMM*, 28 April, 2025, https://admm.asean.org/index.php/about-admm/about-admm.html [date of access: 6.10.2025]; ACICE, *Update on the Information Domain*..., op. cit., p. 2.

[25] Ibidem, pp. 2-4.

The "Ghostwriter" practice further illustrates the coupling of information tactics with the cyber component. Account and website takeovers (the compromise of digital identity) are combined with publishing materials through proxy channels and subsequent amplification on social media. In turn, giving messages an appearance of "authenticity" by impersonating recognizable newsrooms or public offices increases their perceived credibility and strengthens the distribution leverage of both the content "wholesalers" and the local intermediaries responsible for further disseminating the message.[26]

7. Cognitive Warfare: Where Do Proxies "Touch" the Mind?

In the scholarly literature, cognitive warfare – described as a maximalist concept – extends classical understandings of the battlespace to encompass mental and social dimensions.[27] From this perspective, so-called proxy sources function as "cognitive adapters." First, they reduce cognitive dissonance by appealing to the audience's group identity ("this is written by our people"), for example when quasi-portals such as NDP use national symbols and local references to present narratives aligned with Kremlin interests as "patriotic" or "pro-sovereignty." Second, they enhance the credibility of the message by layering intermediaries, which lends information an appearance of ubiquitous presence ("everyone is writing about this"), as seen in the cascading republication of Ghostwriter-related forgeries across minor websites and social media accounts. Third, they activate heuristics of authority, consensus, and availability, thereby lowering the cognitive cost of critically verifying content – for instance, when English-language narratives originating from NewsFront are reproduced by ostensibly independent Western-facing portals and then cited back in national debates as "foreign expert opinions."

Findings from Innovation Hub[28] analyses indicate that the key objective of activities in the realm of cognitive warfare is trust. Its erosion leads to lasting changes in how sources are assessed, thereby increasing the susceptibility of individuals and collectives to manipulation.[29] Empirical observations from the Nordic-Baltic region further suggest that these processes resulted in measurable fluctuations in the perceived risks associated with NATO's presence, migration phenomena, and the narrative of "discrimination against Russian speakers."[30]

[26] RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 2-4, 9-10.

[27] Ch. Deppe, G. S. Schaal, *Cognitive warfare: a conceptual analysis…*, op. cit., pp. 1-3.

[28] The Innovation Hub (IH) is an open community and collaborative platform run by NATO Allied Command Transformation (ACT), bringing together military and civilian experts to collaboratively identify challenges and develop ideas and solutions for the Alliance (including a community, online platform, knowledge base, and the NATO Innovation Challenge). NATO Allied Command Transformation, *Innovation Hub*, https://www.act.nato.int/activities/innovation-hub/ [date of access: 30.09.2025).

[29] F. du Cluzel, *Cognitive warfare…*, op. cit., pp. 7, 27.

[30] NATO StratCom COE, *Russia's footprint in the Nordic-Baltic…*, op. cit., pp. 5-6, 29-30, 35-38, 45-46, 59.

The case studies discussed in this article support this interpretation. In the Ghostwriter operation, the combination of hacked accounts, forged documents, and proxy websites produced a layered structure in which each intermediary appeared to confirm the others, thereby strengthening the perception that "many independent outlets" were reporting the same allegations. In the NewsFront ecosystem, multilingual channels and local proxies provided a similar effect: narratives framed centrally were adapted to national contexts, cited by fringe actors, and occasionally picked up by mainstream outlets as "controversial but relevant views." In both cases, proxies did not simply increase technical reach; they altered how audiences processed information, making disinformation more cognitively "fluent" and less likely to be questioned.

8. Poland and Central Europe: Institutional Frameworks and Resilience Practices

On the day Russia launched its full-scale invasion of Ukraine, CZ.NIC, the Czech association managing the .cz domain registry,[31] after consultations with the competent services, temporarily removed 8 disinformation domains from the DNS. A mechanism for the periodic review of domains was also introduced, along with a time limit on blocking that – if continued beyond three months – requires a decision by the competent authority. Additionally, a public register of domains excluded from the DNS was created, as well as pages listing administratively withdrawn names.[32] As it turned out, such infrastructural interventions (DNS, national registries) can effectively disrupt the content supply chain from intermediaries, provided they are accompanied by transparency and a clear legal basis.[33] In line with these practices, EU sanctions targeting entities that organize the "wholesaling" of narratives (e.g., NewsFront) likewise produced a significant chilling effect and made platform moderation easier.[34]

Thus, the neutralization of proxy sources is possible within the framework of the rule of law, provided that actions are transparent and based on clear legal principles. Unfortunately, reviews of the activities of the vast majority of Western states indicate that there are still significant deficiencies in the areas of rapid attribution and transnational coordination of responses to disinformation and propaganda campaigns.[35]

[31] *About association*, https://www.nic.cz/page/351/ [date of access: 6.10. 2025].

[32] Compare the mechanics of "wholesalers" and local intermediaries: RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 5-6, 9-10, 14-15; NATO StratCom COE, *Russia's footprint in the Nordic-Baltic information environment…*, op. cit., pp. 5, 7, 74; CZ.NIC, *Annual Report 2022*, Prague2023, pp. 7, 26, 75-76, https://www.nic.cz/files/nic/230821_CZNIC_vyrocni_zprava_2022_EN.pdf [date of access: 13.09.2025].

[33] CZ.NIC, *Annual Report 2022*…, op. cit., pp. 5, 26, 74-76.

[34] CEU, *Council Implementing Regulation (EU) 2022/260…*, op. cit., pp. 3-4, 11, 13.

[35] V. Witkowska, V. Krátka Špalková, *Czech Republic: Echoes of Discontent – Far-Right Populism and the Disinformation Dilemma*, [in:] *Russia and the Far-Right…*, op. cit., pp. 253-255.

Against this backdrop, Poland fits into a broader Central European pattern: while there is a strong and enduring consensus on EU and NATO membership, certain soft points of vulnerability remain. These are formed by political and social circles that, for ideological or opportunistic reasons, amplify pro-Kremlin narratives – particularly in the areas of security, energy, and migration. Analyses by the International Centre for Counter-Terrorism (ICCT) indicate that some of these circles function as "narrative laboratories," where specific forms of language and storytelling are tested. Subsequently, often through proxy channels, these narratives permeate the wider public discourse.[36]

Although historical and cultural conditions make Poland a difficult environment for openly pro-Russian initiatives, the risk has not disappeared. Radical communication channels on both ends of the political spectrum, sharing elements of the pro-Kremlin repertoire, function as "proxy nests" and facilitate the transfer of content from "narrative wholesalers" (e.g., NewsFront) into the Polish infosphere, where – under favorable conditions – they undergo further legitimization and diffusion.[37]

9. Methodology for Detecting and Limiting the Influence of Proxy Sources

Effectively mitigating the impact of informational intermediaries requires the integration of network analytics, temporal sensitivity, and content assessment across a multilingual environment. Drawing on the patterns reconstructed in the preceding sections – in particular the sequence placement → layering → integration, the role of legitimization loops, and the regional experiences of DNS-level and sanctions-based interventions – this section translates the article's findings into a set of methodological guidelines for detecting and limiting the influence of proxy sources. In other words, it presents the *practical* implications of the answers to RQ1–RQ3 and of the qualitative verification of H1–H3, outlining how the proposed indicators can inform audits, editorial policies, and regulatory measures in Poland and Central Europe.[38]

[36] P. Witkowski, *Poland: Ex Oriente Lux*, [in:] *Russia and the Far-Right: Insights from Ten European Countries*, eds. K. Rekawek, T. Renard, B. Molas (ed.), The Hague 2024, pp. 305-306, 310-311, 318-319.

[37] For an overview of the limited room for openly pro-Russian initiatives in Poland, rooted in specific historical and cultural conditions, and of the role of fringe far-left and far-right actors and media as key vectors of pro-Kremlin narratives, see: Ł. Wenerski, M. Kacewicz, *Russian soft power in Poland: The Kremlin and pro-Russian organizations*, Budapest 2017, pp. 8-9; A. Yeliseyeu, V. Laputska et al., *Major Pro-Kremlin Disinformation Narratives and Their Transmitters in Poland, Czechia, and Slovakia*, https://www.amo.cz/wp-content/uploads/2023/06/AMO_Pro-Russian-Narratives-in-Czech-Republic-Slovakia-and-Poland.pdf, M. Zadorożna, M. Butuc, *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, "*Security and Defence Quarterly" 2024, no.* 46(2), pp. 47-65; P. Witkowski, *Poland: Ex Oriente Lux*…, op. cit., pp. 305-311, 317-319.

[38] The report identifies the following as "behavioral signatures" of the Ghostwriter campaign: 1. a cyber component preceding the influence phase (gaining access to websites/profiles), 2. a typical focus on

In addition, the audit should also encompass multilingual replication pathways. A typical marker in this regard consists of identical articles appearing in two or three languages within intervals of several hours or days, as well as content indicators – that is, stable narrative frameworks (e.g., "NATO = a threat," "discrimination against Russian speakers," "the EU in collapse") – whose persistent presence has been demonstrated in studies conducted by NB8 NATO StratCom.[39]

The preventive layer should be based on prebunking and so-called "resilience headers," understood as pre-agreed editorial and institutional guidelines that reduce the information system's vulnerability to "content laundering." The ACICE recommendations emphasize, among other things, the avoidance of language that facilitates the legitimization of messages of uncertain provenance, as well as the practice of coordinated silence during periods of heightened sensitivity.[40] A model example in this context remains the response of the electoral commission to the "Macron Leaks" case.[41]

Transferring such measures to the Polish and regional context would require agreed-upon operational protocols among newsrooms, public administration, and platforms, including clear escalation procedures and shared risk lexicons.

The final component of the detection methodology is the response sphere involving platforms and regulators. This includes the mapping of network nodes and the whitelisting of reliable sources (with clearly defined qualification criteria and an appeal mechanism), and – where appropriate and proportionate – short-term

the military thread and targets in Central and Eastern Europe, 3. frequent use of fabricated content provoking official denials, 4. hybrid distribution (inauthentic accounts, email spoofing, impersonation + use of compromised but real websites and accounts), 5. strict "scheduling" of important events (visits, exercises), rarely ad hoc reactions. See: RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 5-7, 8, 10-12, 16-17.

[39] NB8 NATO StratCom – an initiative of eight Nordic-Baltic countries (Denmark, Finland, Iceland, Norway, Sweden, Estonia, Latvia, Lithuania) cooperating in the area of NATO strategic communications, including a coherent alliance narrative, coordination of information and psychological activities, and countering disinformation, including in cooperation with the NATO StratCom Centre of Excellence in Riga. See: NATO StratCom COE, *Russia's Footprint…*, op. cit., pp. 4-5, 54-55, 57, 59, 65-66, 69, 76-77.

[40] ACICE, *Update on the Information Domain…*, op. cit., pp. 4-5.

[41] On Saturday, May 6, 2017, the state Electoral Campaign Control Commission called on the media and citizens not to publish or disseminate leaked materials during the election silence period, reminding them of the possible legal consequences. Following the appeal, "Le Monde," among others, announced that it would not report on the content until the end of the vote. See: E. Schultheis, *The Macron Leaks Probably Came Too Late to Change the French Election*, "The Atlantic" 6 May 2017, https://www.theatlantic.com/international/archive/2017/05/france-macron-leak-hack/525738/ [date of access: 6.10.2025]; J.-B. Vilmer Jeangène, *The "Macron Leaks" Operation: A Post-Mortem*, Washington, DC, Paris2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf [date of access: 6.10.2025]; K. Willsher, *French media warned not to publish Emmanuel Macron leaks*, "The Guardian" 6 May 2017, https://www.theguardian.com/world/2017/may/06/french-warned-not-to-publish-emmanuel-macron-leaks [date of access: 6.10.2025]; REUTERS, *France warns against republishing hacked Macron campaign emails, 6 May 2017*, https://www.reuters.com/article/world/france-warns-against-republishing-hacked-macron-campaign-emails-idUSL9N1GD01N/ [date of access: 6.10.2025].

distribution measures at the level of DNS, hosting, and advertising systems, all based on transparent criteria and appeal procedures. The CZ.NIC experience demonstrates that transparency and the temporary nature of interventions increase public acceptance and reduce the risk of excessive interference, while also serving as an effective tool for disrupting the content supply chains of intermediaries.[42]

10. Conclusions

The aim of this article was to reconstruct the role and operational mechanics of proxy sources in Russian influence operations in Central Europe, with particular emphasis on the sequence of "information laundering" (placement → layering → integration) and the identification of indicators for detecting narrative intermediaries. The research design combined a qualitative review of secondary data with illustrative case studies (Ghostwriter, NewsFront) and an analysis of the regional institutional environment in Poland and its broader Central European context. Methodologically, the study relied on triangulation: cross-linguistic comparisons, reconstruction of citation and link chains, and narrative frame analysis were used to capture both the structural and contextual dimensions of proxy activity.

With regard to RQ1, concerning the role of proxy sources in information laundering, the analysis supports H1. Based on the literature and existing data, it has been shown that proxy sources serve as latent structural carriers, masking the origin of messages and increasing their perceived credibility through legitimization by layers of intermediation. The Ghostwriter campaign and the NewsFront ecosystem illustrate how intermediaries make it more likely that narratives will progress from initial placement on quasi-portals to layering across multiple minor outlets and, ultimately, integration into mainstream debates. Proxies thus do not merely replicate content; they facilitate the transition between phases in the laundering process.

In answering RQ2, which asked about indicators that distinguish proxies from ordinary content replicators, the findings support H2. The most useful markers were found to be: (1) recurrent "link bridges" to a fixed pool of diffusion nodes (e.g., NewsFront, SCF), (2) short-window temporal coincidences of publications across multiple channels, and (3) multilingual replications maintaining a stable narrative core with local shifts in emphasis. The identification of legitimization loops (A→B→C→A) and "boosters" operating in coordinated bursts further refines this picture. Taken together, these indicators can inform practical procedures for detecting and cutting off distribution streams without relying solely on content-based assessments.

[42] CZ.NIC, *Annual Report 2022*…, op. cit., pp. 7, 26, 45, 75-76.

As for RQ3, addressing the linguistic–institutional conditions under which proxy sources are most effective in Poland and the broader Central European region, the evidence lends support to H3. The key enabling factors are the presence of local linguistic intermediaries, who lend the message an appearance of "nativeness," and institutional gaps such as weak editorial verification standards, limited cross-border coordination, and the absence of agreed escalation protocols among newsrooms, platforms, and public authorities. At the same time, regional experiences – notably DNS-level interventions by CZ.NIC and EU sanctions targeting narrative "wholesalers" like NewsFront – indicate that it is possible to effectively limit the influence of proxies within the framework of the rule of law, provided that actions are transparent, proportionate, and accompanied by clear appeal mechanisms.

The qualitative nature of this article, based on secondary data, implies certain limitations. It cannot provide statistically generalizable estimates of the scale of proxy activity, nor does it exhaust the diversity of actors and narratives involved in Russian influence operations in Central and Eastern Europe. Nevertheless, the findings point to several promising directions for future research: network–temporal audits on defined datasets; quantitative measurements of delays between the placement, layering, and integration phases and estimation of "legalization" thresholds; comparative analyses across different languages and audience segments; and evaluation of the effectiveness of regulatory and platform interventions in cutting off "narrative wholesalers."

Building on the results, the article proposes an integrated approach to strengthening resilience against proxy sources. It combines (1) prebunking and "resilience headers" – i.e., agreed editorial guidelines standardizing the presentation of disinformation-related risks; (2) distribution network audits aimed at detecting legitimization loops and linguistic bridges; and (3) transparent, time-limited infrastructural interventions targeting diffusion nodes that act as intermediaries. A resilience ecosystem designed in this way – coherent, measurable, and coordinated – increases the likelihood of neutralizing intermediary sources before their messages reach the phase of mainstream integration, thereby addressing the core objective of cognitive warfare: the contestation and capture of trust.

Bibliography

1. ADMM Cybersecurity & Information Centre of Excellence (ACICE). *Update on the Information Domain — Issue 05/24 (May) Information Laundering*. ASEAN Defence Ministers' Meeting Cybersecurity & Information Centre of Excellence (ACICE), 01 May 2024, https://www.acice-asean.org/files/may_24_info.pdf.

2. ASEAN Defence Ministers' Meeting. *About the ASEAN Defence Ministers' Meeting* [online]. ASEAN Defence Ministers' Meeting (ADMM), 28 April 2025, https://admm.asean.org/index.php/about-admm/about-admm.html.
3. Cao K., Glaister S., Pena A., Rhee D.i, Rong W., Rovalino A., Bishop S., Khanna R., Saini J. S., *Countering Cognitive Warfare: Awareness and Resilience*. *NATO Review*, *20 May 2021*, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.
4. Council of the European Union (CEU), *Council Implementing Regulation (EU) 2022/260 of 23 February 2022 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*, "Official Journal of the European Union" 23 Febr. 2022 L 42..
5. CZ.NIC, *About association*, https://www.nic.cz/page/351/.
6. CZ.NIC, *Annual Report 2022*, https://www.nic.cz/files/nic/230821_CZNIC_vyrocni_zprava_2022_EN.pdf.
7. Deppe C., Schaal G. S., *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept*, "Frontiers in Big Data" 2024, vol. 7, art. 1452129, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full.
8. Digital Forensic Research Lab (DFRLab), *Cyber-enabled disinformation campaign targeted U.S.-Poland alliance*, https://dfrlab.org/2020/06/24/cyber-enabled-disinformation-campaign-targeted-u-s-poland-alliance/.
9. Du Cluzel F., *Cognitive Warfare*, https://www.voltairenet.org/IMG/pdf/20210122_cognitive_warfare.pdf.
10. Gielewska A., *Russia-related accounts and a cyberattack in Poland*, https://vsquare.org/russia-related-accounts-and-a-cyberattack-in-poland/.
11. Google Search Central, *Link best practices for Google*. *Google for Developers*, *4 Febr. 2025*, https://developers.google.com/search/docs/crawling-indexing/links-crawlable?hl=pl.
12. Google Search Central, *Spam policies for Google web search*. *Google for Developers, 10 June 2025*, https://developers.google.com/search/docs/essentials/spam-policies.
13. Google Support, *Manual actions report*. *Search Console Help*, https://support.google.com/webmasters/answer/9044175.
14. Kuśmirek K, *Działania informacyjne Federacji Rosyjskiej w 2023 roku [Information activities of the Russian Federation in 2023]*, "Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30 .
15. Leitenberg M., *Russian disinformation related to biological weapons, 1998–2021*. Annex to: Leitenberg M., *False allegations of biological weapons from Putin's Russia*, "The Nonproliferation Review" 2020, vol. 27, no. 4-6, appendix.
16. NATO Strategic Communications Centre of Excellence (NATO StratCom COE), *Russia's Footprint in the Nordic-Baltic Information Environment: Report 2016/2017*, project director: E. Lange-Ionatamišvili; research team: I. Bērziņa, M. Cepurītis, D. Kaljula, I. Juurvee, Riga 2018.
17. NATO Strategic Communications Centre of Excellence, *Information Laundering in Germany, 2019/2020*, Riga 2020.
18. Pełnomocnik Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP [Government Plenipotentiary for the Security of the Information Space of the Republic of Poland]. *Rosyjska sieć kłamstw [Russia's web of lies]*, 2023 źródło internetowe?.
19. Peoples C., Vaughan-Williams N., *Critical Security Studies: An Introduction – 3rd edition,* Abingdon–New York, 2021.

20. RESET: Digital for Good, *The Ghostwriter Campaign. A Multi-Vector Information Operation: Attempts to Control Its Influence & the Limitations of Current Countermeasures*, London2023, https://www.reset.tech/publications/the-ghostwriter-campaign-report/.
21. REUTERS, *France warns against republishing hacked Macron campaign emails*, *6 May 2017,* https://www.reuters.com/article/world/france-warns-against-republishing-hacked-macron-campaign-emails-idUSL9N1GD01N/.
22. Rzecznik Ministra Koordynatora Służb Specjalnych [Spokesperson for the Minister-Coordinator of Special Services], *Atak dezinformacyjny na Polskę[Disinformation Attack on Poland]*. https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske.
23. Schultheis E., *The Macron Leaks Probably Came Too Late to Change the French Election*, *"The Atlantic"* 6 May 2017, https://www.theatlantic.com/international/archive/2017/05/france-macron-leak-hack/525738/.
24. Sikorski J., *Źródła pośredniczące (proxy sources) w komunikacji politycznej jako narzędzie walki informacyjnej [Proxy sources in political communication as a tool of information warfare]*, [in:] *Komunikowanie polityczne i publiczne w nowych mediach: wybrane przykłady [Political and public communication in new media: selected examples],* eds. A. Grzechynka, K. Szmyd,. Kraków 2025.
25. Sikorski J., *Online analytics portal as an information warfare tool of the Russian Federation and its impact after 24 February 2022: case study: RuBaltic.ru*., "*Sõjateadlane (Estonian Journal of Military Studies)*" 2023, vol. 23.
26. United States Department of State, Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem*, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.
27. United States Department of the Treasury, Office of Foreign Assets Control, *Notice of OFAC Sanctions Actions*, "Federal Register" 20 April 2021 vol. 86, no. 74, (FR Doc. 2021–08087), https://www.govinfo.gov/content/pkg/FR-2021-04-20/pdf/2021-08087.pdf.
28. Vilmer J. J., *The "Macron Leaks" Operation: A Post-Mortem*, Washington, DC, Paris 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.
29. Wenerski Ł., Kacewicz M., *Russian soft power in Poland: The Kremlin and pro-Russian organizations*, Budapest 2017.
30. White B., *An update on doorway pages*, "Google Search Central Blog" 16 March 2015, https://developers.google.com/search/blog/2015/03/an-update-on-doorway-pages.
31. Willsher K., *French media warned not to publish Emmanuel Macron leaks*, "The Guardian" 6 May 2017, https://www.theguardian.com/world/2017/may/06/french-warned-not-to-publish-emmanuel-macron-leaks.
32. Witkowska V., Krátka Špalková V., *Czech Republic: Echoes of Discontent – Far-Right Populism and the Disinformation Dilemma*,[in:] *Russia and the Far-Right: Insights from Ten European Countries*, eds.. K. Rekawek, T. Renard, B. Molas, The Hague2024.
33. Witkowski P., *Poland: Ex Oriente Lux,* [in:] *Russia and the Far-Right: Insights from Ten European Countries,* eds. K. Rekawek, T. Renard, B. Molas, . The Hague 2024.
34. *Yeliseyeu A., Laputska V. ., Havlíček P. , Nemečkayová N., Dubóczi P., Ružičková M., Major Pro-Kremlin Disinformation Narratives and Their Transmitters in Poland, Czechia, and Slovakia*, https://www.amo.cz/wp-content/uploads/2023/06/AMO_Pro-Russian-Narratives-in-Czech-Republic-Slovakia-and-Poland.pdf.
35. Zadorożna M., Butuc M., *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, "*Security and Defence Quarterly" 2024,* 46(2).