Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

Resilience Factors in Influence Operations in the Context of CTI Analysis

Piotr FILIPKOWSKI
pfilip@sgh.waw.pl (Corresponding author)
https://orcid.org/0000-0003-1464-4977
SGH Warsaw School of Economics, Warsaw, Poland

Ignas KALPOKAS
ikalpo@sgh.waw.pl; ignas.kalpokas@vdu.lt
https://orcid.org/0000-0003-1110-5185
SGH Warsaw School of Economics, Warsaw, Poland;
Vytautas Magnus University, Kaunas, Lithuania

Received: 8 August 2025 | Revised: 24 November 2025
Accepted: 18 December 2025 | Available online: 30 December 2025

This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/

Abstract

This paper investigates the strategic deployment of disinformation as a tool of influence operations, focusing on Russian campaigns targeting perceptions of Ukrainian refugees in Poland and the EU. Utilizing the Diamond Model for Influence Operations and supported by Cyber Threat Intelligence analysis from Recorded Future, the study identifies key actors, audiences, capabilities, and infrastructure involved in these malign efforts. The authors argue that disinformation is not merely a spread of falsehoods, but a deliberate manipulation of narratives designed to exploit technological affordances and societal vulnerabilities. The research highlights how emotionally charged content, algorithmic amplification, and coordinated bot activity contribute to the virality and perceived credibility of disinformation. The case illustrates how Russia seeks to fracture European solidarity, delegitimize Ukraine, and erode public support for humanitarian and military aid. The findings underscore the importance of societal resilience, advocating for enhanced media literacy, institutional trust, and multi-level countermeasures. Ultimately, the paper concludes that combating influence operations requires a holistic approach that integrates technological, regulatory, and educational strategies to mitigate the impact of strategically crafted disinformation.

Keywords: cyber threat intelligence, defense strategy, disinformation, influence operations, narrative warfare, societal safety

1. Introduction

In today's information ecosystem, the spread of disinformation has emerged as not only an internal threat to societies and their political cohesion but also as a challenge to geopolitical stability. This article delves into such disinformation, highlighting the strategic, technological, and informational dynamics of the latter, demonstrating that disinformation is not merely a byproduct (communication noise or human error) but, instead, a tool wielded by state and non-state actors to shape perceptions, manipulate public opinion, and destabilize adversary societies by way of deliberate crafting and dissemination of narratives, i.e. coherent and emotionally resonant stories that override factuality and appeal to audience identities, biases, concerns, and beliefs.

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

A crucial role here is played by the digital-first information environment, in which the reach of content is amplified by social media platforms and algorithmic curation of information that foster the formation of echo chambers and filter bubbles. Given that content virality has become a proxy for credibility, falsehoods gain traction not necessarily due to their truth-value but because of their novelty, emotional appeal, and perceived popularity. In this way, not only is susceptibility to misleading information increased, but also trust in legitimate institutions is eroded, social solidarity is undermined, and polarization is facilitated. Adversaries can thus exploit technological affordances for large-scale malign influence operations.

Disinformation, through its effects on public opinion and, consequently, policy preferences and electoral choices of citizens, constitutes a major threat to today's democracies. Three sets of factors contributing to its spread can be identified. One is technological: today's environment is structurally conducive to the dissemination of such content. The second is strategic: certain countries seem to be deliberately including information warfare into their arsenal of means for the achievement of geopolitical gains, such as Russia's attempts to spread disinformation in the context of its aggression against Ukraine. The third one is the information factor: attack narratives aim to disrupt the rationality of actions by building a false belief in the understanding of the injustice of the world and control over life. Of course, the three are not separate and should be analyzed together.

Disinformation campaigns are not random or free-standing: they tend to align with geopolitical objectives. Here, Russia is a paramount example. Building on Soviet-era doctrines of reflexive control and psychological manipulation, Russia makes use of an infrastructure comprising state media, embassies, bot networks, and proxy influencers to execute coordinated influence operations. In the context of Russia's aggression against Ukraine, disinformation has been mobilized to delegitimize Ukraine, fracture European solidarity – particularly in frontline states like Poland.

This article offers an analysis of one such narrative: the portrayal of Ukrainian refugees as a problem for Poland and other EU countries. Drawing on the Diamond Model of Influence Operations, it identifies the actors, audiences, capabilities, and infrastructure underpinning this narrative. The article demonstrates how content is weaponized to trigger societal divisions, foster resentment, and, ultimately, to erode support for Ukraine. These efforts are situated within a broader information warfare strategy, highlighting the interplay of content, technology, and social vulnerabilities. Hence, this article contributes to a deeper understanding of how modern information operations function as instruments of power.

2. Narrative as a key message payload

Of particular importance is the narrativization of truth claims. Building a narrative or jumping onto the bandwagon of existing narratives allows for stronger attraction and retention of attention than standalone messages would. This feature is crucial in today's oversaturated information environment. Simultaneously, such narrativization also strengthens the appeal of falsehoods by seemingly making them part of something significantly larger. Crucially, of all sense-making structures, narrative carries the greatest weight, trumping factuality and verifiable information. In fact, '[m]ore and more pure information or facts only muddles our understanding of the world', thereby increasing the desire for clear-cut stories (Holmstrom, 2015, p. 121). This is particularly acute in new and/or challenging situations when previous frames of reference cannot be automatically applied or when one is unsure what to make out of new developments, because suddenly 'there is a void that needs to be filled' (Holmstrom, 2015, p. 121). Under such circumstances, people immediately find themselves in a situation of a struggle over meaning, whereby '[i]f one side fails to provide a meaningful narrative, others will fill the void' – after all, 'people need simple stories that provide them with relevant information, talking points, and an explanation of how the topic in question fits into their worldview' (Holmstrom, 2015, p. 121). The specific case analyzed in this article (Russia's war against Ukraine and the influx of refugees) straddles across these levels as a source of international insecurity (necessitating narratives of how to function in the new environment), a challenge to national decision-making (necessitating a narrative of how the government should adapt its policies), and a challenge to local communities (how to adapt to the influx of refugees). What ensues, then, is a struggle for narrative, not only among well-meaning and constructively concerned groups but also involving actors partaking in disinformation campaigns (see also Kalpokas, 2024).

Particularly in cases when trust in the media and other mainstream information sources is low, individuals tend to self-sort into pre-existing camps while treating information that falls outside already internalized narratives as malicious, regardless of its veracity – this has been observed, among others, in case of Russia's war against Ukraine, where positions and news source selection has been found to significantly correlate with pre-existing opinions and adherence to older historical, political, and national narratives (Hameleers et al. 2024). Hence, one can see that once a narrative has taken hold, it becomes true through its own effects, fixing 'what were just vague inclinations into solid ideas or "truths"; this, however, rarely happens in a vacuum as an effective narrative typically 'plays on feelings and simmering passions already present, reinforcing opinions, hardening prevailing stereotypes and creating automatic reflexes' (Holmstrom, 2015, p. 123). Crucially, a narrative, as a concentration and fixation of meaning that seemingly explains the world, can either grow out of a community's shared way of existence or be strategically manufactured on that same collective basis by actors at home and abroad.

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

The preceding is particularly relevant in times of information overabundance, whereby selection from available content has become the main challenge (Vaidhyanathan, 2018, p. 80). A narrative structure of the world allows one to (relatively) easily slot the available content into a (relatively) neat worldview without putting in significant time and effort. Moreover, narratives provide orientation and comfort by explaining not only the world in general but also its actual or perceived injustices that matter to people. This function can be performed even by false narratives, e.g. conspiracy theories, that, despite their non-factuality, 'connect people, give meaning to experienced disparities and corruption in society' (Harambam et al. 2022, p. 785). Hence, if being wrong allows audiences to feel in control while also forging positive collective identities, then, at least within such communities, there is no demand for truthful information (Goldthwaite Young, 2023).

3. Attack infrastructure – social media – screen time

Narratives thrive on shared meanings, stereotypes, biases, etc., while also being collectively produced and reinforced. This is where the technological dimension kicks in. One factor here is social media and screen time as an attack infrastructure. Crucially, 'social media affords collective expression – understood as deliberately connecting to an assumed audience with similar beliefs by making use of shared symbolic resources' (Literat & Kligler-Vilenchik, 2019, p. 2002). The latter statement might seem paradoxical – after all, it is more common to refer to social media as vehicles for personal self-expression. Nevertheless, since no self can be substantiated without a shared structure of meaning, this interpersonal dimension becomes key. Thus, context digital platforms 'do not reflect the social: they produce the social structures we live in' (van Dijck, Poell & de Waal, 2018, p. 2; see also Simon, 2024). Here, a value split is clearly visible: on the one hand, through the use of Artificial Intelligence tools, platforms 'can select the relevant item to put in front of the user's eyes' because matching content with user preferences increases user satisfaction and retention; on the other hand, there is a notable shift of power and priorities as 'information that is relevant for the public debate is not defined by the exchange of views and opinions but machines' (De Gregorio, 2022. p. 174). Platforms thus take over information selection and supply and do so proactively, i.e., by way of foreseeing and, if necessary, molding audience opinions (Johnen & Samogyi, 2024; Simon, 2024), thereby performing public functions (including structuring the information environment and governing social encounters) without the limitations and transparency obligations that have been set over time to limit the power of public authorities – despite having comparable influence (see, e.g., De Gregorio, 2022).

4. Rationality on the web

Simultaneously, platform-curated content becomes the window to the world and a source of common sense for a significant part of today's citizens (Simon, 2024) – a trend that is further strengthened by the ability of communicators (marketing, political, and the like) to directly target individuals who are likely, based on the data available, to be susceptible to the promoted message (Nayak & Walton, 2024). No less importantly, audiences seem to develop a perception that if something is relevant and important, it will, sooner or later, show up in their news feed, thereby becoming significantly more passive in intentional information searching behaviors (Lin et al. 2024). These processes have conventionally been claimed to cause (or at least significantly contribute to) the so-called filter-bubble effect, thereby locking users in environments dominated by a single viewpoint, regardless of its veracity: not only users select whom to connect to online, what groups to join, what content to consume, etc. but also the content governance algorithms further enclose them in information cocoons by only showing users content that they are going to like. Moreover, relationality is a crucial factor in this respect as people tend to opt for content that seems to evoke consensus, particularly by affirming collective beliefs (Chadwick & Stanyer, 2022, p. 9).

However, the collective/relational dimension is not only a source of (often fake) meaning – it is also generally open to manipulation, including so-called astroturfing campaigns that aim to imitate grassroots support for a particular cause or idea. By way of coordinating among multiple (inauthentic) accounts, such campaigns involve posting, sharing, liking, and commenting on messages, (fake) news stories, memes, and other content to create the impression of popular support (see, e.g., Zerback & Töpfl, 2022; Chan, 2024). The goal is not necessarily to convince target audiences of the truthfulness of the message but, instead, of its popularity, because popularity itself can become a criterion for truthfulness. In other cases, general erosion of trust in any content can be a sufficient goal in itself (Zerback & Töpfl, 2022, pp. 400–401; Chan, 2024). For example, anti-Ukrainian disinformation could be successful not only if it convinces audiences of Russia's narrative, but also if it makes people less willing to support any side.

Still, one must not to give in to 'a baseless nostalgia for a by-gone era characterized by truth and reason' and to the 'moral panics' of technologically determined disintegration of truth (Harjuniemi, 2022, p. 279).

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

5. Technologically enhanced propaganda

While both state and non-state actors engage in information warfare, when discussing such threats, Russia typically comes to the fore because of both the scale of its efforts and its long-standing treatment of information as a strategic asset. It is notable that already in Soviet strategic thought, disinformation and reflexive control of the target populations had played a prominent role at least since the 1960s (Bachmann et al., 2023). In more recent times, digital (primarily social media-based) instances of Russian propaganda and other manipulative efforts have been observed on multiple occasions, implying that social media has essentially become a domain of modern information conflict – one used to divide and influence public opinion (Geissler et al., 2023, p. 2). In the context of Russia's war on Ukraine, the key purpose of disinformation has been to crack Western support for Ukraine (at both political and societal levels) and generally discrediting Ukraine and its people (Bachmann et al., 2023), including the Ukrainian refugees who had fled to other European countries. Hence, to provide a more in-depth snapshot of such disinformation efforts, this article delves into the specificities of disinformation campaigns against Ukrainian refugees in Poland – a country that is not only a key strategic ally of Ukraine but also the destination for many such refugees.

Previous research indicates repeated exposure as having significant effects on belief formation (that is, the more often individuals encounter some claims, the more likely they are to come round to believing them), particularly if such claims happen to align with one's ideological convictions and other prior beliefs (Soares et al., 2023). Likewise, macro-level factors, such as historical experience, socio-material situation, and nationally dominant views and concerns means that such susceptibility to disinformation narratives, including Russia's attempts to discredit Ukraine and Ukrainians, relies not only on individual but also on country-wide factors (Wenzel et al., 2024), making it reasonable to study disinformation campaigns on a national (and not only individual or group) level.

The coordinated manner of such efforts is often evidenced by the patterns of disinformation's emergence: it tends to be neither sporadic nor particularly diverse but, instead, appears in waves, whereby particular audiences become bombarded by a mass of messages, all promoting the same or similar narrative and serving a single aim; such waves can typically be described by two key traits: 'content quality (thematization, focus on certain protagonists, genre forms, and data formats) and intensity (massiveness of messages)' (Krainikova & Prokopenko, 2023, p. 23). Another sign of coordination has been the distribution of bot-powered content, which has been spread in clear clusters in countries of strategic interest to Russia in its aggression against Ukraine, for example, South Africa or India (Geissler et al., 2023, p. 16). It is reasonable to expect that similar patterns may appear in strategically selected European countries.

An important role here is played by the echo chambers and filter bubbles on social media, particularly if the groups targeted can be defined by characteristics assisting self-selection (ethnicity is one example, but various socio-material and demographic categories could potentially be used as well); such characteristics are then used to stress differences between the rest of society and an 'out' group, which is targeted for demonization, thus increasing polarization. There already is research suggesting that this strategy has been heavily used by Russia to stir opinion against Ukraine and Ukrainians (Sablina, 2023). Hence, patterns of amplification are another aspect to monitor in disinformation campaigns.

6. Cyber Threat Intelligence Analysis – Diamond model for influence operations

An example of influence operations in the media is the activity of Russian state bodies.

a. Narrative: Refugees from Ukraine are a problem for Poland and other EU countries – Diamond's Core

This narrative is part of a broader disinformation strategy aiming to delegitimize Ukraine, legitimize Russia's aggression against Ukraine, undermine public support for refugees from Ukraine, and weaken EU member state solidarity. It also aims to divide public opinion, shifting blame away from Russian aggression by framing the humanitarian response as a failure of Western governance. The central narrative seeks to portray Ukrainian refugees as a significant burden to both Poland and other EU countries (EUvsDisinfo, 2025a; ISD, 2024; NATO, 2025).

It suggests that refugees from Ukraine are overburdening the host states, causing social, economic, and cultural instability. Also, it posits the influx of displaced individuals from Ukraine as causing social, economic and security tensions. The message often implies that Ukrainian refugees contribute to rising crime rates, instability in social services, and internal division within the EU (NASK, 2025; FEPS, 2022; Demagog, 2025; InvestigateBel, 2025).

Tactics include highlighting alleged crimes by refugees, economic burden, and the idea that the EU prioritizes Ukrainians over locals. Some of the most common claims include that refugees are putting pressure on public services like healthcare, housing or education (Atlantic Council – DFRLab, 2023; FEPS, 2022; Mentzelopoulou & Orav, 2025).

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

b. Influencer – Socio-political Axis

The primary influencer is the Russian state, i.e. the Russian regime under Vladimir Putin through state institutions (foreign and interior ministries, secret services, military) with the aim of weakening the solidarity of EU countries with Ukraine through setting up and sponsoring influence operations and thus achieving military and ideological goals in the war against Ukraine (and the West) (EUvsDisinfo, 2025c; SGDSN, 2025).

The most active official institutions involved in these efforts include the Russian government and the Russian Embassy in Poland, which disseminate official narratives through diplomatic communication channels and public statements. Supporting this effort are Russian state-controlled media outlets such as RT and Sputnik, which publish content designed to amplify anti-refugee sentiment (Myth Detector, 2023; Konkret24, 2025; EUvsDisinfo, 2024; Warsaw Institute, 2023).

Pro-Russian online communities and disinformation actors – particularly those linked to operations like the "Doppelgänger" campaign – further disseminate the narrative through fake social media accounts and coordinated messaging tactics (Alaphilippe et al., 2022; Federal Foreign Office, 2024).

Moreover, operations can be carried out by institutions such as secret services and cyber units, but also by the following groups in return for sponsorship or the granting of other privileges (CISA, 2024; CISA, 2025; EUvsDisinfo, 2025b, U.S. Department of Justice, 2024):

- other state-affiliated/sponsored Russian or international actors/ civil society organizers (e.g., pro-Russian hacker/activist groups) who deliberately share the narrative on their (local or international) channels to support the Russian state in its goals and possibly also to make a name for themselves there (in terms of powerful connections);
- politically "neutral" criminal groups or individuals who provide disinformation as a service for financial reasons.

c. Audience – Socio-political Axis

The targeted audiences for this narrative are carefully chosen to maximize disruption. In this case, the primary focus is on Polish citizens. These also include citizens who are economically vulnerable, politically conservative, or skeptical of multiculturalism (EU DisinfoLab, 2025; EDMO, 2022; DFRLab, 2022).

A broader audience includes citizens with existing anti-immigrant sentiments, who may be more receptive to messaging that blames refugees for systemic issues, particularly in societies of host countries that are otherwise politically Ukraine-friendly (Neidhardt, 2022; Joint Research Centre, 2023; Poland Insight, 2025).

Another group susceptible to manipulation are global societies outside Europe/the West or Russia, promoting a narrative that Europe is overwhelmed with the reception of refugees and is no longer safe, e.g., for foreign students or tourists, thus being aimed at long-term (reputational and economic) damage to Western countries (Joint Research Centre, 2023; Neidhardt, 2022; AFP Fact Check, 2022).

To amplify the message, Russian-speaking emigre communities in countries that support Ukraine are also included in the audience (Plaza, 2024; Ukrainian Institute, 2022).

To reinforce the validity of Russian actions in Ukraine, the audience also includes Russian society. The desired effect is to amplify the narrative that Ukrainians are 'bad people' and either do not deserve or need support (because Russia is 'liberating' them from a 'fascist' regime) (ISD, 2022; Lough et al., 2014).

A broader vulnerable group is social media users – particularly susceptible to algorithmic echo chambers and viral disinformation – who can become unwitting propagators (DFRLab, 2022; HarfangLab, 2024; Chawryło, 2024).

Additionally, policymakers in the EU and NATO and media figures are targeted to influence public discourse and potentially shift immigration or foreign policy decisions (Ronzaud et al., 2023; Sessa & Miguel (2024).

Finally, international observers are exposed to the narrative to undermine the EU's image as a unified and humanitarian actor (Council of the European Union, 2025).

d. Capabilities – Technical Axis

Influencers share links to related Russian websites, disinformation websites, or, for example, Russia-friendly niche newspapers, news platforms / social media pages, as well as videos on platforms (Alaphilippe et al., 2022; U.S. Cyber Command, 2024; RFE/RL Schemes, 2024).

Depending on the target group, the narrative is increasingly disseminated on television (older sections of the population) or in comments on social media (younger to middle-aged population) or multipliers share it in community groups, e.g., on Telegram (NATO StratCom COE, 2024; ISD, 2022; EU Neighbours East, 2024).

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

The dissemination takes place mainly in local (European) languages, as well as in English and Russian in Russia-friendly media. Emotional engagement is achieved through provocative headlines and cartoons, targeted messages via social media. They use emotionally charged visuals and selective statistics to distort reality (EUvsDisinfo, 2022; Neidhardt & Butcher, 2022).

Information tools that Russia uses to carry out the influence operation include diplomatic messaging through embassy statements or press releases, and pro-Russian media, including websites and newspapers. In addition, they spread fake news, use bots and social media trolls (U.S. Department of State, 2020; Marigliano, Ng, & Carley, 2024; University of Adelaide, 2022).

On the technical axis, the campaign's capabilities include disinformation tactics such as emotional manipulation, selective truth distortion, and amplification of isolated negative incidents involving refugees. These are often framed as representative of a wider problem (DISA, 2025; Rogalewicz, 2023; EDMO, 2025).

Influencers use access to multilingual media platforms, bot networks and amplification via Telegram, VKontakte, and anonymous forums (Dergacheva, 2025; Alaphilippe et al., 2022).

e. Infrastructure – Technical Axis

The infrastructure includes Russian state media (e.g., RT, Sputnik), embassy websites and social media channels, fringe news platforms, and Telegram groups (U.S. Department of State, 2022; Boucher & Fridman, 2025; DFRLab, 2022). Together, these elements form a coordinated influence operation that exploits social vulnerabilities to advance geopolitical objectives by discrediting Western support for Ukraine and deepening divisions within European societies (Alaphilippe et al., 2022; Federal Foreign Office, 2024; EDMO, 2022).

The infrastructure used to support this influence campaign is sophisticated and multi-layered (Sekoia, 2024). Bot networks and troll farms are employed to amplify posts and create the illusion of widespread support or concern by malicious comments (UK FCDO, 2022; Mustafa et al., 2025). Deepfake videos and AI-generated content further enhance the campaign's credibility and emotional appeal (SGDSN, 2025; NATO StratCom COE, 2024; Harding, 2024). Fake news websites, crafted to resemble legitimate Western outlets, are also used to host and circulate disinformation narratives that align with the campaign's goals (Alaphilippe et al., 2022; Osadchuk & Carvin, 2024; U.S. Cyber Command, 2024).

f. Case Study: Refugees from Ukraine are a problem for Poland and other EU countries

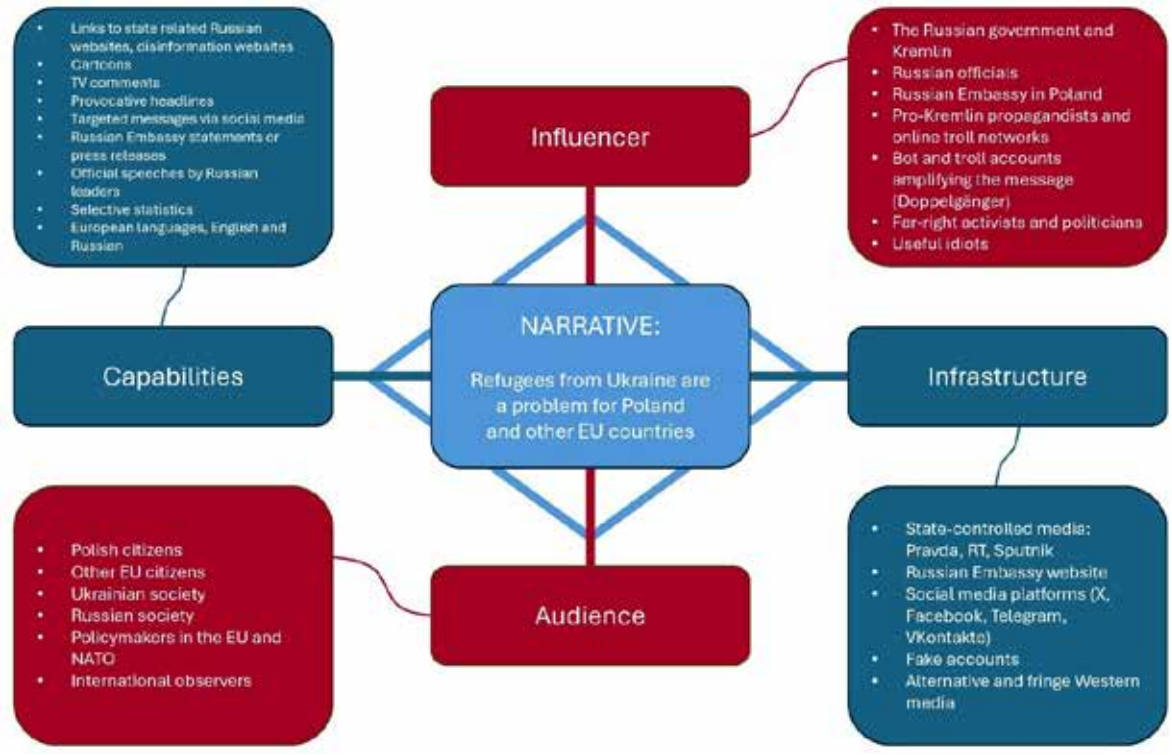

Figure 1. A list of detected indicators related to a Russian state-sponsored influence campaign against Ukrainian society. Source: the authors' own work.

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

7. Conclusions

The present disinformation landscape is characterized by intentionality, scale, and sophistication. As demonstrated, disinformation should not be understood simplistically as merely the spread of falsehoods in a chaotic information environment – instead, it is a strategic tool that builds on societal vulnerabilities, existing technological infrastructures and affordances, and societally rooted narrative structures. Russia has institutionalized disinformation to influence foreign and domestic audiences alike. During its war against Ukraine, these efforts are especially evident in the targeting of public perceptions regarding Ukrainian refugees in countries such as Poland.

Through the narrative that frames Ukrainian refugees as a burden, Russia seeks to weaken European solidarity, foment division within host societies, and delegitimize both Ukrainian resistance and Western support. These campaigns are carried out by employing a coordinated network of state media, bots, social media influencers, and emotionally evocative content that taps into pre-existing fears, biases, and grievances. In the same vein, the interplay between technological affordances and social dynamics enhances the effectiveness of influence operations, meaning that narratives, more than facts, shape perceived realities. Crucially, disinformation does not require audiences to fully believe such falsehoods but, instead, success can be achieved by amplifying doubt, confusion, and social fragmentation. Overall, then, countering such threats demands a complex response that encompasses technological, regulatory, societal, and educational in order to build and foster societal resilience.

Acknowledgements
The research was conducted in the Virtual Laboratory of the Institute of Information Systems and Digital Economy with the technological support of Recorded Future Platform and reports from the Insikt Group for the purpose of Cybersecurity classes at the Warsaw School of Economics. The research was based on the methodology presented by Recorded Future White Papers Resources in *The Diamond Model for Influence Operations Analysis*.

Declaration of interest
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. AFP Fact Check. (2022). *These images were taken in Melilla, and do not show African migrants fleeing Ukraine*. https://factcheck.afp.com/doc.afp.com.326C2MD
2. Alaphilippe, A., Machado, G., Miguel, R., & Poldi, F. (2022). *Doppelganger – Media clones serving Russian propaganda*. EU DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf
3. Atanasova, A., Lesplingart, A., Poldi, F. & Kuster, G. (2024). *Operation Overload*. Check First. https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf
4. Atlantic Council – DFRLab. (2023). *Pro Kremlin sources amplify forged diplomatic letters targeting Ukrainian refugees*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-pro-kremlin-sources-amplify-forged-diplomatic-letters-targeting-ukrainian-refugees
5. Bachmann, S.-D. D., Putter, D. & Duczynski, G. (2023). Hybrid Warfare and Disinformation: A Ukraine War Perspective. *Global Policy*, 14, pp. 858–869.
6. Boucher, J.-C., & Fridman, O. (2025). *Russia's worldwide information manipulations on Telegram and X: A pilot study*. Community of Democracies. https://community-democracies.org/app/uploads/2025/01/Russias-Information-Manipulation-Telegram-and-X.pdf
7. Chadwick, A. & Stanyer, J. (2022). Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Toward a Holistic Framework. *Communication Theory*, 32, pp. 1–24.
8. Chan, J. (2024). Online Astroturfing: A Problem Beyond Disinformation. *Philosophy and Social Criticism*, *50*(3), pp. 507–528.
9. Chavane, C., Amaury, G. & Seznec K. (2023). *Master of Puppets: Uncovering the Doppelganger pro-Russian influence campaign*. Sekoia, https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/#h-victimology-objective-and-attribution
10. Chawryło, K. (2024). *'Doppelgänger': The pattern of Russia's anti Western influence operation*. Ośrodek Studiów Wschodnich. https://www.osw.waw.pl/en/publikacje/analyses/2024-09-13/doppelganger-pattern-russias-anti-western-influence-operation
11. CISA. (2024). *Russian military cyber actors target US and global critical infrastructure (AA24 249A)*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a
12. CISA. (2025). *Pro Russia hacktivists conduct opportunistic attacks against US and global critical infrastructure (AA25 343A)*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

13. Council of the European Union. (2025). *How the EU helps refugees from Ukraine*. Consilium. https://www.consilium.europa.eu/en/policies/refugee-inflow-from-ukraine/
14. De Gregorio, G. (2022). *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge and New York: Cambridge University Press.
15. Demagog. (2025). *Antyukraińska propaganda: sierpień–listopad 2025. Raport*. Demagog. https://demagog.org.pl/analizy_i_raporty/antyukrainska-propaganda-sierpien-listopad-2025-raport-demagoga-i-imm
16. Dergacheva, D. (2025). 'One crap news per week': How Kremlin propaganda works on VKontakte social media platforms. *Global Voices*. https://globalvoices.org/2025/04/09/one-crap-news-per-week-how-kremlin-propaganda-works-on-vkontakte-social-media-platforms
17. DFRLab (Digital Forensic Research Lab). (2022). *Polish language Telegram channels spread anti refugee narratives*. Atlantic Council. https://dfrlab.org/2022/05/31/polish-language-telegram-channels-spread-anti-refugee-narratives
18. DFRLab (Digital Forensic Research Lab). (2022). *How Russia attempt to widen its arsenal of pro-war propaganda*. DFRLab. https://medium.com/dfrlab/how-russia-attempts-to-widen-its-arsenal-of-pro-war-propaganda-c0a6181b4efb
19. DISA Press Room. (2025). *Investigation reveals Russian disinformation campaign targeting Ukrainian refugees in Poland ahead of June referendum*. https://disa.org/investigation-reveals-russian-disinformation-campaign-targeting-ukrainian-refugees-in-poland-ahead-of-june-referendum
20. EDMO (2022). *Ukrainian refugees and disinformation: Situation in Poland, Hungary, Slovakia and Romania*. https://edmo.eu/publications/ukrainian-refugees-and-disinformation-situation-in-poland-hungary-slovakia-and-romania
21. EU DisinfoLab. (2025, October 27). *The disinformation landscape in Poland*. https://www.disinfo.eu/publications/disinformation-landscape-in-poland
22. EU Neighbours East. (2024). *Disinformation on Telegram: How Russian propaganda works in temporarily occupied territories*. https://euneighbourseast.eu/news/stories/disinformation-on-telegram-how-russian-propaganda-works-in-temporarily-occupied-territories
23. EuvsDisinfo. (2021). *Główny cel kremlowskiej dezinformacji*. https://euvsdisinfo.eu/pl/glowny-cel-kremlowskiej-dezinformacji
24. EUvsDisinfo. (2022). *Disinfo: Ukrainian refugees provoked a record outbreak of HIV in Poland*. https://euvsdisinfo.eu/report/ukrainian-refugees-provoked-a-record-outbreak-of-hiv-in-poland
25. EUvsDisinfo. (2024). *The Kremlin's disaster disinformation exploits in Poland*. https://euvsdisinfo.eu/the-kremlins-disaster-disinformation-exploits-in-poland
26. EUvsDisinfo. (2025a). *Disinformation cases database*. https://euvsdisinfo.eu/disinformation-cases/?text=refugees%20ukraine&_=1765546642123
27. EUvsDisinfo. (2025b). *The rise of the disinformation for hire industry*. EUvsDisinfo (East StratCom Task Force). https://euvsdisinfo.eu/the-rise-of-the-disinformation-for-hire-industry
28. EUvsDisinfo. (2025c). *UKRAINE*. https://euvsdisinfo.eu/ukraine
29. Federal Foreign Office. (2024). *Germany targeted by the pro Russian disinformation campaign "Doppelgänger": Technical report*. https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1-data.pdf
30. FEPS (Foundation for European Progressive Studies). (2022). *Disinformation on refugees from Ukraine: Boosting Europe's resilience after Russia's invasion*. https://feps-europe.eu/wp-content/uploads/2022/12/PS-Disinformation.pdf
31. Geissler, D. et al. (2023). Russian Propaganda on Social Media During the 2022 Invasion of Ukraine. *EPJ Data Science*, 12, pp. 1–20.
32. Goldthwaite Young, D. (2023). *Wrong: How Media, Politics, and Identity Drive Our Appetite for Misinformation*. Boston (MA): Johns Hopkins University Press.
33. Hameleers, M. et al. (2024). Mistakenly Misinformed or Intentionally Deceived? Mis- and Disinformation Perceptions on the Russian War in Ukraine Among Citizens in 19 Countries. *European Journal of Political Research*, *63*(4), pp. 1642–1654.
34. Harambam, J., Grusauskaite, K. & de Wildt, L. (2022). Poly-Truth, or the Limits of Pluralism: Popular Debates on Conspiracy Theories in a Post-Truth Era. *Public Understanding of Science*, *31*(6), pp. 784–798.
35. Harding, E. (2024). *A Russian bot farm used AI to lie to Americans. What now?* Center for Strategic & International Studies. https://www.csis.org/analysis/russian-bot-farm-used-ai-lie-americans-what-now
36. HarfangLab. (2024). *Mid year Doppelgänger information operations in Europe and the US*. https://harfanglab.io/insidethelab/doppelganger-operations-europe-us
37. Harjuniemi, T. (2022). Post-Truth, Fake News and the Liberal 'Regime of Truth': The Double Movement Between Lippmann and Hayek. *European Journal of Communication*, *37*(3), pp. 269–283.
38. Holmstrom, M. (2015). The Narrative and Social Media. *Defence Strategic Communications*, *1*(1), pp. 119–133.

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

39. InvestigateBel. (2025). *Crime among Ukrainian refugees in Europe: the facts*. https://investigatebel.org/en/analytics/ukrainian-refugees-crime-europe-statistics
40. ISD (Institute for Strategic Dialogue). (2022). *A false picture for many audiences: How Russian-language pro Kremlin Telegram channels spread propaganda and disinformation about refugees from Ukraine*. https://www.isdglobal.org/digital_dispatches/a-false-picture-for-many-audiences-how-russian-language-pro-kremlin-telegram-channels-spread-propaganda-and-disinformation-about-refugees-from-ukraine
41. ISD (Institute for Strategic Dialogue). (2024). *Two Years On: An analysis of Russian state and pro Kremlin information warfare in the context of the invasion of Ukraine*. https://www.isdglobal.org/wp-content/uploads/2024/02/Two-Years-on_ISD.pdf
42. Johnen, J. and Samogyi, R. (2024). Deceptive Features on Platforms. *The Economic Journal*, 134, pp. 2470–2493.
43. Joint Research Centre. (2023). *Solidarity with people displaced from Ukraine: Communication, fighting disinformation are key*. European Commission. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/solidarity-people-displaced-ukraine-2023-09-15_en
44. Kalpokas, I. (2024). Post-Truth and Information Warfare in Their Technological Context. *Applied Cybersecurity & Internet Governance*, *3*(2), pp. 99–121.
45. Konkret24. (2025). *Sieć prorosyjskich portali oplata Polskę. Oto 10 przykładów*. https://konkret24.tvn24.pl/polska/siec-prorosyjskich-portali-oplata-polske-oto-10-przykladow-st8372898
46. Krainikova, T., & Prokopenko, S. (2023). Waves of Disinformation in the Hybrid Russian-Ukrainian War. *Current Issues of Mass Communication*, 33, pp. 12–25.
47. Lin, Y. ir kt. (2024). Understanding the Effects of News-Finds-Me Perception on Health Knowledge and Information Seeking During Public Health Crises. *Health Communication*, *39*(2), pp. 352–362.
48. Literat, I. & Kligler-Vilenchik, N. (2019). Youth Collective Political Expression on Social Media: The Role of Affordances and Memetic Dimensions for Voicing Political Views. *New Media & Society*, *21*(9), pp. 1988–2009.
49. Lough, J., Lutsevych, O., Pomerantsev, P., Secrieru, S., & Shekhovtsov, A. (2014). *Russian influence abroad: Non state actors and propaganda [Meeting summary]*. Chatham House. https://www.chathamhouse.org/sites/default/files/field/field_document/20141024RussianInfluenceAbroad.pdf
50. Marigliano, R., Ng, L. H. X., & Carley, K. M. (2024). Analyzing digital propaganda and conflict rhetoric: A study on Russia's bot driven campaigns and counter narratives during the Ukraine crisis. *Social Network Analysis and Mining*, 14, 170. https://doi.org/10.1007/s13278-024-01322-w
51. Mentzelopoulou, M. M., & Orav, A. (2025). *Displaced Ukrainians: Challenges and outlook for integration in the EU (EPRS Briefing, PE 769.497)*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769497/EPRS_BRI(2025)769497_EN.pdf
52. Mustafa, H., Luczak Roesch, M., & Johnstone, D. (2025). Conceptualizing the evolving nature of computational propaganda: A systematic literature review. Oxford Internet Institute. *Annals of the International Communication Association*, *49*(1), 45–60. https://doi.org/10.1093/anncom/wlaf001
53. Myth Detector. (2023). *Twitter accounts of Russian diplomatic missions at the forefront of spreading disinformation*. https://mythdetector.com/en/twitter-accounts-of-russian-diplomatic-missions-at-the-forefront-of-spreading-disinformation/
54. NASK. (2025). *Jak dezinformacja kształtuje nasze postrzeganie Ukrainy?* https://www.nask.pl/aktualnosci/jak-dezinformacja-ksztaltuje-nasze-postrzeganie-ukrainy
55. NATO StratCom COE. (2024). *Russia's information influence operations in the Nordic–Baltic region*. NATO Strategic Communications Centre of Excellence https://stratcomcoe.org/publications/russias-information-influence-operations-in-the-nordic-baltic-region/314
56. NATO StratCom COE. (2024). *Virtual Manipulation Brief 2024/1: Hijacking reality – the increased role of generative AI in Russian propaganda*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/virtual-manipulation-brief-20241-hijacking-reality-the-increased-role-of-generative-ai-in-russian-propaganda/307
57. NATO. (2025). *NATO's approach to counter information threats*. North Atlantic Treaty Organization. https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats
58. Nayak, B. S. & Walton, N. (2024). The Future of Platforms, Big Data and New Forms of Capital Accumulation. *Information Technology & People*, *37*(2), pp. 662–676.
59. Neidhardt, A.-H. (2022). *Disinformation on refugees from Ukraine: Boosting Europe's resilience after Russia's invasion*. European Policy Centre. https://www.epc.eu/publication/Disinformation-on-refugees-from-Ukraine-Boosting-Europes-resilience-4c56f8
60. Neidhardt, A. H., & Butcher, P. (2022). *Disinformation on migration: How lies, half truths, and mischaracterizations spread*. Migration Policy Institute. https://www.migrationpolicy.org/article/how-disinformation-fake-news-migration-spreads

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

61. Osadchuk, R., & Carvin, A. (2024). *Doppelganger: How Russia mimicked real news sites and created fake ones to target US audiences*. DFRLab – Atlantic Council. https://dfrlab.org/2024/09/18/doppelganger-us-election
62. Plaza, J. (2024). *"Rossotrudnichestvo" as a Russian tool of influence in the Czech Republic*. Warsaw Institute. https://warsawinstitute.org/rossotrudnichestvo-as-a-russian-tool-of-influence-in-the-czech-republic
63. Poland Insight. (2025, December 2). *Anti Ukrainian disinformation surges in Poland as media and EU officials call for coordinated action*.https://polandinsight.com/anti-ukrainian-disinformation-surges-in-poland-as-media-and-eu-officials-call-for-coordinated-action-86125
64. Recorded Future. *The Diamond Model for Influence Operations Analysis*. White Papers Resources. https://assets.recordedfuture.com/Whitepapers/diamond-model-influence-operations-analysis.pdf
65. Recorded Future. *Ukraine Intelligence Kit*. Support Resource Centers: Russian Aggression in Ukraine: Ukraine Intelligence Kit. https://support.recordedfuture.com/hc/article_attachments/18053521209747
66. RFE/RL (Radio Free Europe/Radio Liberty) – Schemes. (2024). *Leaked records detail vast Russian influence campaign targeting Ukraine, EU*. https://www.rferl.org/a/russia-ukraine-disinformation-propaganda-campaign/33123498.html
67. Rogalewicz, M. (2023). *Russian disinformation about Ukrainian refugees in Poland*. Warsaw Institute. https://warsawinstitute.org/russian-disinformation-about-ukrainian-refugees-in-poland
68. Ronzaud, L., Carter, J. A., & Williams, T. (2023). *Summit Old, Summit New: Russia linked actors leverage new and old tactics in influence operations targeting online conversations about NATO summit*. Graphika. https://public-assets.graphika.com/reports/graphika_report_summit_old_summit_new.pdf
69. Sablina, L. (2023). The Role of Social Media in Facilitating Minority Mobilisation: The Russian-Language Pro-War Movement in Germany Amid the Invasion of Ukraine. *Nations and Nationalism*, 29, pp. 1422–1438.
70. Sekoia. (2024). *Master of Puppets: Uncovering the DoppelGänger pro Russian influence campaign*. https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign
71. Sessa, M. G., & Miguel, R. (2024). *The Doppelganger case: Assessment of platform regulation on the EU disinformation environment*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/the-doppelganger-case-assessment-of-platform-regulation-on-the-eu-disinformation-environment/304
72. SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale). (2025). *Analysis of the Russian information manipulation set Storm-1516*. General Secretariat for Defence and National Security. https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf
73. SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale). (2025). *War in Ukraine: Three years of Russian information operations (Version 1.0) [Report]*. General Secretariat for Defence and National Security. https://www.sgdsn.gouv.fr/files/2025-02/20250224_TLP-CLEAR_NP_SGDSN_VIGINUM_War%20in%20Ukraine_Three%20years%20of%20Russian%20information%20operations_1.0_VF.pdf
74. Simon, F. M. (2024). Escape Me If You Can: How AI Reshapes News Organisations' Dependency on Platform Companies. *Digital Journalism*, *12*(2), pp. 149–170.
75. Służby specjalne (2022). *Hybrydowy atak na Polskę*, GOV.PL. https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske, access 20.07.2025.
76. Soares, F. B., Gruzd, A. & Mai, P. (2023). Falling for Russian Propaganda: Understanding the Factors that Contribute to Belief in Pro-Kremlin Disinformation on Social Media. *Social Media + Society*, doi: 10.1177/20563051231220330
77. U.S. Cyber Command. (2024). *Russian disinformation campaign "DoppelGänger" unmasked: A web of deception*. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception
78. U.S. Department of Justice. (2024). *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
79. U.S. Department of Justice. (2024). *US Social Media Influencers Network*. https://www.justice.gov/archives/opa/media/1366191/dl
80. U.S. Department of State – Global Engagement Center. (2020). *Russia's pillars of disinformation and propaganda*. https://2021-2025.state.gov/russias-pillars-of-disinformation-and-propaganda-report
81. U.S. Department of State – Global Engagement Center. (2022). *Report: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem*. https://2021-2025.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem
82. UK Foreign, Commonwealth & Development Office (UK FCDO). (2022, May 1). *UK exposes sick Russian troll factory plaguing social media with Kremlin propaganda*. https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda

Safety & Defense 11(2) (2025)
DOI https://doi.org/10.37105/sd.268

83. Ukrainian Institute. (2022). *"The Russian Flag Will Be Flown Wherever Russian Is Spoken": "Russkiy Mir" Foundation – study*. https://ui.org.ua/en/sectors-en/russkiy-mir-foundation-2/
84. University of Adelaide. (2022). *Bots manipulate public opinion in Russia–Ukraine conflict*. https://www.adelaide.edu.au/newsroom/news/list/2022/09/08/bots-manipulate-public-opinion-in-russia-ukraine-conflict
85. Vaidhyanathan, S. (2018). *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford and New York: Oxford University Press.
86. van Dijck, J., Poell, T. & de Waal, M. (2018). *The Platform Society: Public Values in a Connective World*. Oxford and New York: Oxford University Press.
87. Wenzel, M. et al. (2024). The Penetration of Russian Disinformation Related to the War in Ukraine: Evidence from Poland, the Czech Republic and Slovakia. *International Political Science Review*, *45*(2), pp. 192–208.
88. Zerback, T. and Töpfl, F. (2022). Forged Examples as Disinformation: The Biasing Effects of Political Astroturfing Comments on Public Opinion Perceptions and How to Prevent Them. *Political Psychology*, *43*(3), pp. 399–418.