Simone Castagna[*]
Giulia Porrino[**]
Federico Borgonovo[***]

The Italian pro-Russia digital ecosystem on Telegram

Abstract

The dissemination of pro-Russia ideologies and associated visual motifs has become widespread and transversal, encompassing various communities within the digital ecosystem. This trend has been linked to the related cognitive warfare that targets public opinion, manipulates information, and undermines the credibility of democratic institutions. Regarding the Italian context, the period from 2019 to 2023 saw a dramatic increase in the number of actors promoting pro-Russia narratives. They included members of the no-vax and no-greenpass movements, conspiracy theorists, far-right organizations, neo-Nazi groups, and ultras. Concurrently, the digital ecosystem has contributed the spread of violent content and anti-establishment propaganda online. In order to identify and explore the Italian digital ecosystem affected by pro-Russia ideologies, this study exploits a combination of exponential discriminative snowball sampling and social network analysis techniques on the Telegram instant messaging service. Through this approach, this research provides insight into the organizational structure and dynamics of the network, identifying key actors and their relationships, and the dissemination patterns of pro-Russia and anti-establishment propaganda. This study proposes a new research methodology to study digital ecosystems permeated by cognitive warfare campaigns and provides a deeper understanding of the mechanisms through which such content is propagated, enabling the development of effective strategies for countering disinformation and promoting fact-based discourse.

Key words: Russia, disinformation, cognitive warfare, Italian, social network analysis

[*] Simone Castagna, Ianalyst In The Cyber, Milano.

[**] Giulia Porrino, ITSTIME, Università Cattolica del Sacro Cuore, Intern.

[***] Dr. Federico Borgonovo, research-analyst at ITSTIME, Università Cattolica del Sacro Cuore, Department of Sociology, e-mail: federico.borgonovo@unicatt.it, ORCID: 0000-0002-0028-6737.

Introduction

On February 24, 2022, Russia invaded Ukraine[1], extending the Russo--Ukrainian conflict that had started with the annexation of Crimea in 2014[2]. Currently, the conflict has resulted in significant energy, material, and food shortages[3], and one of the worst refugee crises in history, with more than 8 million Ukrainians fleeing their homes[4]. The United Nations General Assembly condemned the invasion in Resolution ES-11/1[5], which was endorsed by 141 countries, while five countries voting against (Belarus, Democratic People's Republic of Korea, Eritrea, Russian Federation, Syrian Arab Republic), and 35 countries abstaining (e.g., China, India, Iran, Iraq, Pakistan).

A general concern is that the tactics of cognitive warfare, in form of large-scale Russian propaganda campaigns, are being employed to manipulate the narrative around the conflict. Actually, the Russian government's approach has been to enact new legislation and use its influence over traditional media outlets, with the aim of encouraging citizens to support the ongoing war effort. This has resulted in domestic media outlets being compelled to conform to the official narrative[6]. Conversely, Russia propaganda is also suspected of attempting to manipulate the view of people outside Russia, primarily by leveraging social media to spread anti-Western sentiment[7]. Actually, even though Russian propaganda has been observed in several Western countries during previous conflicts[8], there is no robust empirical evidence of its use from the 2022 invasion of Ukraine.

[1] *Situation in Ukraine*, Security Council, 7683th meeting, https://www.unmultimedia.org/avlibrary/asset/1613/1613953/ [access: 28.04.2016].

[2] Ibidem.

[3] I. Liadze, C. Macchiarelli, P. Mortimer-Lee, P.S. Juanino, *The economic costs of the Russia-Ukraine conflict*, London 2022, p. 12.

[4] *Ukraine Refugee Situation*, https://data.unhcr.org/en/situations/ukraine [access: 22.03.2023].

[5] *Resolution adopted by the general Assembly on 2 March 2022*, UN Doc A/RES/ES-11/1, 2022, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/293/36/PDF/N2229336.pdf?OpenElement [dostęp: 22.03.2023].

[6] I. Aieva, J.D. Moffitt, K.M. Carley, *How disinformation operations against Russian opposition leader Alexei Navalny influence the international audience on Twitter*, „Social Network Analysis and Mining" 2022, vol. 12, no. 1, p. 80; W. Sloane, *Putin cracks down on media*, „British Journalism Review" 2022, vol. 33, no. 3, p. 19–22.

[7] S. Sanovich, S. Woolley, P. Howard, *Computational propaganda in Russia: The origins of digital misinformation*, „Working Paper" 2017, no. 3, p. 1–25; I. Yablokov, *Russian disinformation finds fertile ground in the West*, „Nature Human Behaviour" 2022, vol. 6, no. 6, p. 766–767.

[8] I. Aieva, J.D. Moffitt, K.M. Carley, op. cit., p. 80; Y. Golovchenko, *Measuring the scope of pro-Kremlin disinformation on Twitter*, „Humanities and Social Sciences Communications" 2020, vol. 7, no. 1, p. 176.

It is therefore necessary to conduct further research on the extent and impact of pro-Russia propaganda during the 2022 invasion of Ukraine. Specifically, the authors are not aware of any academic studies quantitatively exploring the effects of cognitive warfare on Telegram digital communities and their dynamics. This claim is supported by extensive research through various search engines such as Google Scholar, Connected Papers, Scinapse, and Scopus. Building from these considerations, this research proposes an exploratory investigation of the Italian digital ecosystem on Telegram spreading pro-Russia propaganda as a case study. Through the social network analysis technique, it is intended to contribute in understanding what the dimension of the Italian frontline in the Russian cognitive warfare is, as well as the dynamics and influence of the actors populating it. The findings will highlight for the first time how the Russian propaganda spread throughout a nation and provide interesting outputs for potential counter-offensive effort. In general, this research also aims to propose a research methodology based on social network analysis to study digital ecosystems affected by cognitive warfare activities.

The paper is organised into four sections. The next section provides an overview of the latest research in both the literature on Russian cognitive warfare and studies of hard-to-reach communities on Telegram. The second section argues in favour of using snowball sampling and social network analysis methodologies to explore the Italian pro-Russia digital ecosystem on Telegram, as well as describing the exploited data. The third section reports the results of the performed analyses. The fourth section discusses the results considering both prior studies on Russian cognitive warfare and future research developments.

Literature reviev

In modern warfare theory, cognitive domain has emerged as a distinct field, alongside the traditional domains of land, maritime, air, space, and the interconnecting cyber domain[9]. Although there is no generally accepted definition

[9] T. Bucher, A. Helmond, *The Affordances of Social Media Platforms* [in:] *The SAGE Handbook of Social Media*, eds. J. Burgess, A. Marwick, T. Poell, Thousand Oaks 2018, p. 233–253; B. Claverie, F. Du Cluzel, *Cognitive Warfare: The Advent of the Concept of „Cognitics" in the Field of Warfare* [in:] *Cognitive Warfare: The Future of Cognitive Dominance*, eds. B. Claverie, B. Prébot, N. Buchler, F. du Cluzel, Paris 2022, p. 2, 1–7; P. Ottewer, *Defining the Cognitive Domain*, https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/ [access: 7.12.2020].

of cognitive warfare, its essence and capacity are contained in the following excerpt: „in cognitive warfare, the human mind becomes the battlefield. The aim is to change not only what people think, but how they think and act. […] In its extreme form, it has the potential to fracture and fragment an entire society, so that it no longer has the collective will to resist an adversary's intentions"[10].

Even before the Ukrainian invasion in 2022, other geopolitical events have demonstrated the importance and effectiveness of this new domain in shaping public opinion, influencing national behaviours, and achieving strategic objectives[11]. Specifically, the Russian government seems to be aware of these concepts and capabilities, as demonstrated by the cognitive warfare campaigns attributed to the Internet Research Agency. This organisation is suspected of being behind coordinated social media campaigns to influence public opinion already during the 2014 Russian-Ukrainian conflict[12]. Among many cases, the Internet Research Agency sought to influence the outcomes of the 2016 U.S. presidential election[13], even though its influence American voting behaviour has been doubted[14].

[10] K. Cao et al., *Countering cognitive warfare: Awareness and resilience*, NATO Review, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [access: 20.05.2021].

[11] A. Arif, L.G. Stewart, K. Starbird, *Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse*, „Proceedings of the ACM on Human-Computer Interaction" 2018, vol. 2, p. 1–27; E. Ferrara, *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election*, https://doi.org/10.48550/ARXIV.1707.00086 [access: 26.04.2023]; M. Grčar, D. Cherepnalkoski, I. Mozetič, P. Kralj Novak, *Stance and influence of Twitter users regarding the Brexit referendum*, „Computational Social Networks" 2017, vol. 4, no. 1, p. 6; T.C. Hung, T.W. Hung, *How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars*, „Journal of Global Security Studies" 2022, vol. 7, no. 4.

[12] L. Doroshenko, J. Lukito, *Trollfare: Russia's disinformation campaign during military conflict in Ukraine*, „International Journal of Communication" 2021, no. 15, p. 28; Y. Golovchenko, op. cit., p. 176; idem, M. Hartmann, R. Adler-Nissen, *State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation*, „International Affairs" 2018, vol. 94, no. 5, p. 975–994.

[13] A. Badawy, E. Ferrara, K. Lerman, *Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign* [in:] *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Lyon 2018, p. 258–265; U. Dutta et al., *Analyzing Twitter Users' Behavior Before and After Contact by the Russia's Internet Research Agency*, „Proceedings of the ACM on Human-Computer Interaction" 2021, no. 5 (CSCW1), p. 1–24; A.M. Guess, B. Nyhan, J. Reifler, *Exposure to untrustworthy websites in the 2016 US election*, „Nature Human Behaviour" 2020, vol. 4, no. 5, p. 472–480; L. Luceri, S. Giordano, E. Ferrara, *Detecting Troll Behavior via Inverse Reinforcement Learning: A Case Study of Russian Trolls in the 2016 US Election*, „Proceedings of the International AAAI Conference on Web and Social Media" 2020, no. 14, p. 417–427.

[14] G. Eady et al., *Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior*, „Nature Communications" 2023, vol. 14, no. 1, p. 62.

On the other side, the dearth of scientific research into extremist digital communities on Telegram, the lack of first-hand information regarding morphology and dynamics of these communities, and the convergence of extremist's networks on Telegram, all suggest that there is also research needing when it comes to understanding how extremist actors communicate and connect with each other on social media. In particular, a milestone in research on the topic was laid when it has been observed that communities' social and relational setting evolve continuously, also driven by the development of new technologies that influence and often facilitate their connections, interactions, and communications[15]. Indeed, with the proliferation of digital platforms and social media, communication facilitated by technology has become integrated into online and offline everyday activities[16]. However, all studies on extremist digital communities have focused exclusively on mainstream social media platforms, specifically Facebook and Twitter. Yet, these platforms have recently begun banning far-right, jihadist, and other categories of extremist actors[17]. As a result, extremist communities and their surrounding individuals "migrate" to other platforms. For instance, after a wave of bans on Twitter in 2016, Qanon and other far-right users started moving to a social network named Gab[18]. Similarly, Telegram messaging application gained popularity among various extremist networks in 2019[19].

In general, Telegram has become attractive for different types of user engagements[20]. By providing enhanced privacy and anonymity, along with the opportunity to gain publicity through channels and coordinate and mobilize

[15] J. Postill, S. Pink, *Social Media Ethnography: The Digital Researcher in a Messy Web*, „Media International Australia" 2012, no. 1, p. 123–134.

[16] A.C. Garcia, A.I. Standlee, J. Bechkoff, Y. Cui, *Ethnographic Approaches to the Internet and Computer-Mediated Communication*, „Journal of Contemporary Ethnography" 2009, vol. 38, no. 1, p. 52–84.

[17] K. Paul, J. Waterson, *Facebook bans Alex Jones, Milo Yiannopoulos and other far-right figures*. „The Guardian", https://www.theguardian.com/technology/2019/may/02/facebook-ban-alex-jones-milo-yiannopoulos [access: 2.05.2019].

[18] J. Wilson, *Gab: Alt-right's social media alternative attracts users banned from Twitter*, „The Guardian", https://www.theguardian.com/media/2016/nov/17/gab-alt-right-social-media-twitter [access: 17.11.2016].

[19] R. Rogers, *Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media*, „European Journal of Communication" 2020, vol. 35, no. 3, p. 213–229; T. Owen, *How Telegram Became White Nationalists' Go-To Messaging Platform. In Vice*, https://www.vice.com/en/article/59nk3a/how-telegram-became-white-nationalists-go-to-messaging-platform [access: 24.04.2023].

[20] T. Bucher, A. Helmond, *The Affordances of Social Media Platforms* [in:] *The SAGE Handbook of Social Media*, eds. J. Burgess, A. Marwick, T. Poell, Thousand Oaks 2018, p. 233–253.

through groups, Telegram presents a solution to address the security versus efficiency trade-off[21]. This issue is being faced by terrorist and extremist online communities as they strive to balance their propaganda efforts with the operational activities[22]. It is therefore inevitable that users who seek to spread propaganda and mobilize individual while maintaining their anonymity are attracted by Telegram features. This user demographic encompasses a wide range, from demonstrators to paramilitary groups and terrorist networks, including Islamic State[23].

The aforementioned studies have distinctly aided the advance the understanding of cognitive warfare theory, on Russian campaigns in this domain, and the investigation of hard-to-reach communities on Telegram. Still, it is suggested that there is a significant research gap concerning the quantitative estimation of the cognitive warfare battlefield, dynamics, and impacts. In this paper, it is argued that research on cognitive warfare must not be limited to mainstream social media platforms. These are often chosen because it is easier to gather relevant information and metadata necessary for analysis in them. Precisely for this reason and basing on the literature presented in this section, it was decided that is necessary to restrict the scope of this research exclusively to communities on Telegram.

Data and methods

Data collection

The data were collected through Telegram's integrated „export chat history" function using exponential discriminative snowball sampling[24]. The initial

[21] C. Morselli, C. Giguère, K. Petit, *The efficiency/security trade-off in criminal networks*, „Social Networks" 2007, vol. 29, no. 1, p. 143–153.

[22] A. Urman, S. Katz, *What they do in the shadows: Examining the far-right networks on Telegram*, „Information, Communication & Society" 2022, vol. 25, no. 7, p. 904–923.

[23] L. Cinciripini, F. Borgonovo, M. Zaliani, *Propaganda weaponisation: Lo sfruttamento della pandemia da parte di attori non statali*, „Call for Papers #CASD" 2020, no. 1; M. Krona, *Mediating Islamic State\textbar Collaborative Media Practices and Interconnected Digital Strategies of Islamic State (IS) and Pro-IS Supporter Networks on Telegram*, „International Journal of Communication" 2020, no. 14, p. 23.

[24] R. Atkinson, J. Flint, *Accessing hidden and hard-to-reach populations: Snowball research strategies*, „Social Research Update" 2021, vol. 33, no. 1, p. 1–4; F. Baltar, I. Brunet, *Social research 2.0: Virtual snowball sampling method using Facebook*, „Internet Research" 2012,

seed, which will not be mentioned for security reasons, is a channel connected to PMC Wagner that gathers open source intelligence on Ukrainian fighters. It was chosen because it can effectively reach hidden populations with chased properties[25]. In fact, it was observed that several Italian users shared Italian pro-Russia channels in the chat linked to the starting seed. Messages from these Italian pro-Russia channels were collected, and then forwards from other channels were extracted. Channel connections are represented through forwards, which were chosen because they indicate both the sources of the information and their dissemination by channels. Thus, the inherent characteristics of forwards data present two distinct roles, namely the forwarder and the forwarded, resulting in a directed network structure.

Since the starting channel was not chosen at random, the nature of the sampling procedure introduced some distortions in the data collection. This will be discussed in detail in the Potential Methodological Limitations subsection.

Overall, data were collected from a total of 20 public channels, spanning a time period ranging from the creation of the first considered channel in October 2019 to February 2023. Subsequently, a citation network was assembled by extracting all forwards from the twenty channels. Forwards consist of direct reposts from other channels, without consideration for the sentiment of the referred content. The resulting citation network has 1291 nodes and 20 edges weighted by the number of forwards between channels, while the total number of forwards (unweighted edges) was found to be 25889.

Methods

From a methodological point of view, this research follows the steps of studies that have relied on network analysis to examine interconnections between different hard-to-reach communities and accounts[26]. Specifically, the network was collapsed into a single snapshot, ignoring the temporal

vol. 22, no. 1, p. 57–74; L.A. Goodman, *Snowball Sampling*, „The Annals of Mathematical Statistics" 1961, vol. 32, no. 1, p. 148–170.

[25] I. Etikan, *Comparision of Snowball Sampling and Sequential Sampling Technique*, „Biometrics & Biostatistics International Journal" 2016, vol. 3, no. 1.

[26] C. Froio, B. Ganesh, *The transnationalisation of far right discourse on Twitter: Issues and actors that cross borders in Western European democracies*, „European Societies" 2019, vol. 24, no. 4, p. 513–539; M. Krona, op. cit., p. 23; D. O'Callaghan et al., *An Analysis of Interactions within and between Extreme Right Communities in Social Media* [in:] *Ubiquitous Social Media*

dimension. Following the application of the community detection algorithm[27], descriptive network statistics were examined at network, subgroup, and node level in order to highlight the dynamics of the ecosystem and its main actors. In particular, the community detection algorithm makes it possible to separate the network into groups of nodes that are more closely related to nodes within a given community than to nodes outside it. In this specific research context, this means that channels and groups within a given community are more likely to forward and be forwarded by other channels and groups within that community.

Potential methodological limitations

Even though snowball sampling and social network analysis are effective methods in social research to investigate hard-to-reach communities, they are not without limitations. The main limitation of snowball sampling relevant to this research is the sample selection bias[28]. This bias arises because individuals tend to interact with others who share their characteristics and beliefs. While the presented case study aims for sample homogeneity, it cannot be excluded that there are other Italian communities that are affected by pro-Russia propaganda but are not detected because they significantly differ from those identified in one or more characteristics.

On the other hand, social network analysis has relevant limitations related to the challenges associated with the technique (e.g., community clustering, opinion leader identification, stance detection) and the type and quality of the data gathered[29]. All these limitations are even more relevant in light of Telegram's privacy orientation, described in detail in the literature review section.

Analysis, eds. M. Atzmueller, A. Chin, D. Helic, A. Hotho, Berlin; Heidelberg 2013, p. 88–107; A. Urman, S. Katz, op. cit., p. 904–923.

[27] V.D. Blondel, J.L. Guillaume, R. Lambiotte, E. Lefebvre, *Fast unfolding of communities in large networks*, „Journal of Statistical Mechanics: Theory and Experiment" 2008, no. 10, p. 8.

[28] F. Baltar, I. Brunet, op. cit., p. 57–74; T. Dosek, *Snowball Sampling and Facebook: How Social Media Can Help Access Hard-to-Reach Populations*, „PS: Political Science & Politics" 2021, vol. 54, no. 4, p. 651–655.

[29] U. Can, B. Alatas, *A new direction in social network analysis: Online social network analysis problems and applications*, „Physica A: Statistical Mechanics and Its Applications" 2019, vol. 535 (C); D. Knoke, S. Yang, *In Social network analysis*, 3 ed., Thousand Oaks 2019.

Results and discussion

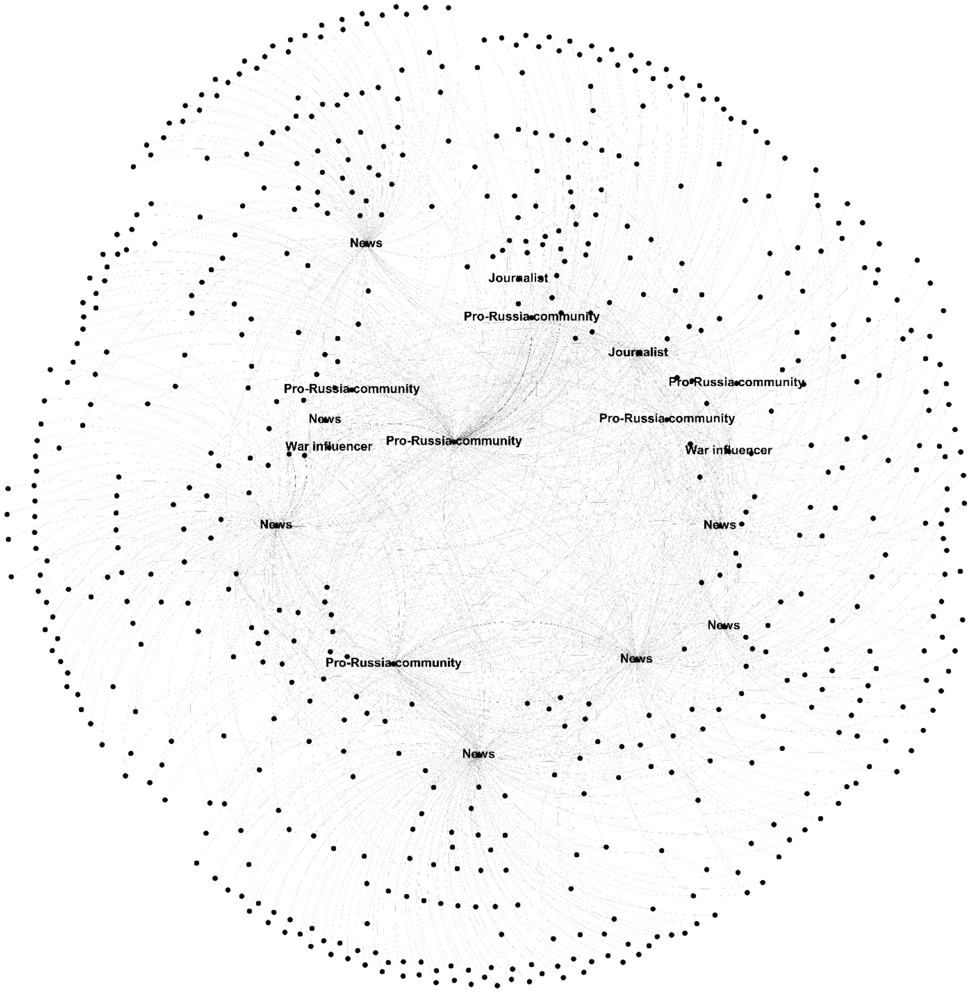
Whole network level analysis

The network presented in Figure 1 provide a first visual representation of the structure and properties of the Italian pro-Russia digital ecosystem on Telegram. It illustrates the inter-channel connections and the direction of information between channel without considering the time component. The representation of the network in Figure 1 was rendered using a force directed ForceAtlas algorithm implemented in Gephi[30]. For security reasons, the names of the channels have been anonymized in all the figures.

At the whole network level, it is significant to analyse the density of the network. This metric reflects the overall level of connectivity among its constituent nodes. It is calculated by dividing the sum of existing connections by the maximum number of possible connections, yielding a proportion that ranges from 0 to 1. In the present research, the density of the network was computed as 0,004, indicating a low degree of interconnectivity.

Such a low-density value implies that information transmission between individual channels within the network may be suboptimal, as many potential paths for information flow may not exist. However, the network is also likely to be more resilient to disruptions and damage than networks with higher densities. Specifically, the removal of a few channels would not significantly impair the overall functioning of the network, as there are relatively few connections to begin with.

[30] M. Bastian, S. Heymann, M. Jacomy, *Gephi: An Open Source Software for Exploring and Manipulating Networks*, „Proceedings of the International AAAI Conference on Web and Social Media" 2009, vol. 3, no. 1, p. 361–362.



Source: own elaboration.

Fig. 1. Network layout of the Italian pro-Russia digital ecosystem on Telegram

Subgroup level analysis

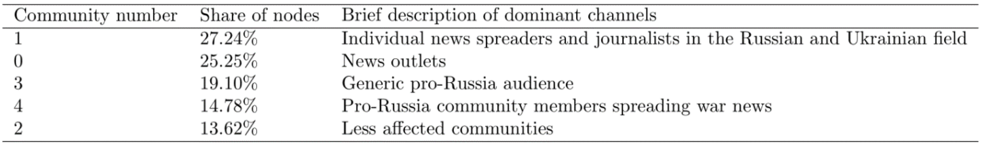
The Italian pro-Russia digital ecosystem on Telegram has been analysed applying the community detection algorithm[31] to the networks' final snapshot, which identifies 5 distinct communities and calculated a modularity score of 0,458. According to Newman and Girvan (2004), higher modularity scores

[31] V.D. Blondel, op. cit., p. 8.

indicate a stronger network structure, and in this case the modularity metric does not suggests that the network has a well-defined community structure. This finding is consistent with the decentralized and fragmented nature of similar networks observed on other platforms[32].

Table 1 presents the distribution of communities detected in the network. The size of each community is expressed as the percentage of nodes it encompasses. Additionally, it is provided a brief overview of each community. References to channel names included in each community have not been included for security reasons.

Table 1. Distribution of communities in the network by share of nodes



Community number	Share of nodes	Brief description of dominant channels
1	27.24%	Individual news spreaders and journalists in the Russian and Ukrainian field
0	25.25%	News outlets
3	19.10%	Generic pro-Russia audience
4	14.78%	Pro-Russia community members spreading war news
2	13.62%	Less affected communities

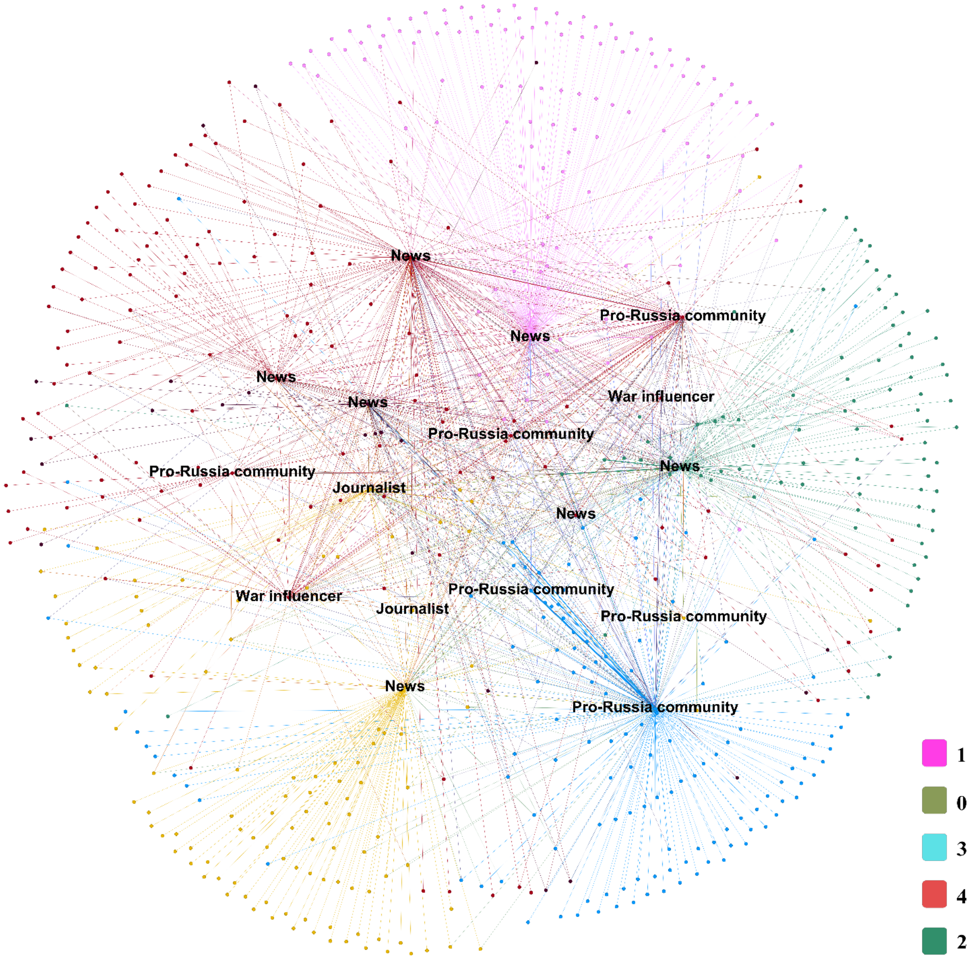
In order to facilitate the interpretation, the „Community number” column serves as a reference system to match each community's location within the network represented in Figure 2 using the provided colour legend. The representation of the network in Figure 1 was rendered using a force directed ForceAtlas algorithm implemented in Gephi[33].

The concept of modularity class extends beyond identifying specific communities within the network, but also offers insight into the type of content disseminated within these groups. In particular, community number 1 (see Table 1) is predominantly composed by individual news spreaders and journalists within the Russian and Ukrainian fields, whose primary product is news dissemination. Conversely, community number 0 is composed of news outlets, namely media houses that focus on the dissemination of news updates in a non-personalized format. On the other side, community number 3 is representative of those subgroups known to side with Russia, probably heavily influenced by pro-Russia propaganda. Community number 4 represents a small, hybrid, subgroup that predominantly relays news about the war but also ties to the communities

[32] C. Froio, B. Ganesh, op. cit., p. 513–539; O. Klein, J. Muis, *Online discontent: Comparing Western European far-right groups on Facebook*, „European Societies” 2019, vol. 21, no. 4, p. 540–562; D. O'Callaghan et al., op. cit., p. 88–107.

[33] M. Bastian et al., op. cit., p. 361–362.

affected by pro-Russia propaganda. Finally, community class 2 represents the smallest in the network, comprising the remainder of the network with low content identification and weak ties to pro-Russia narratives.

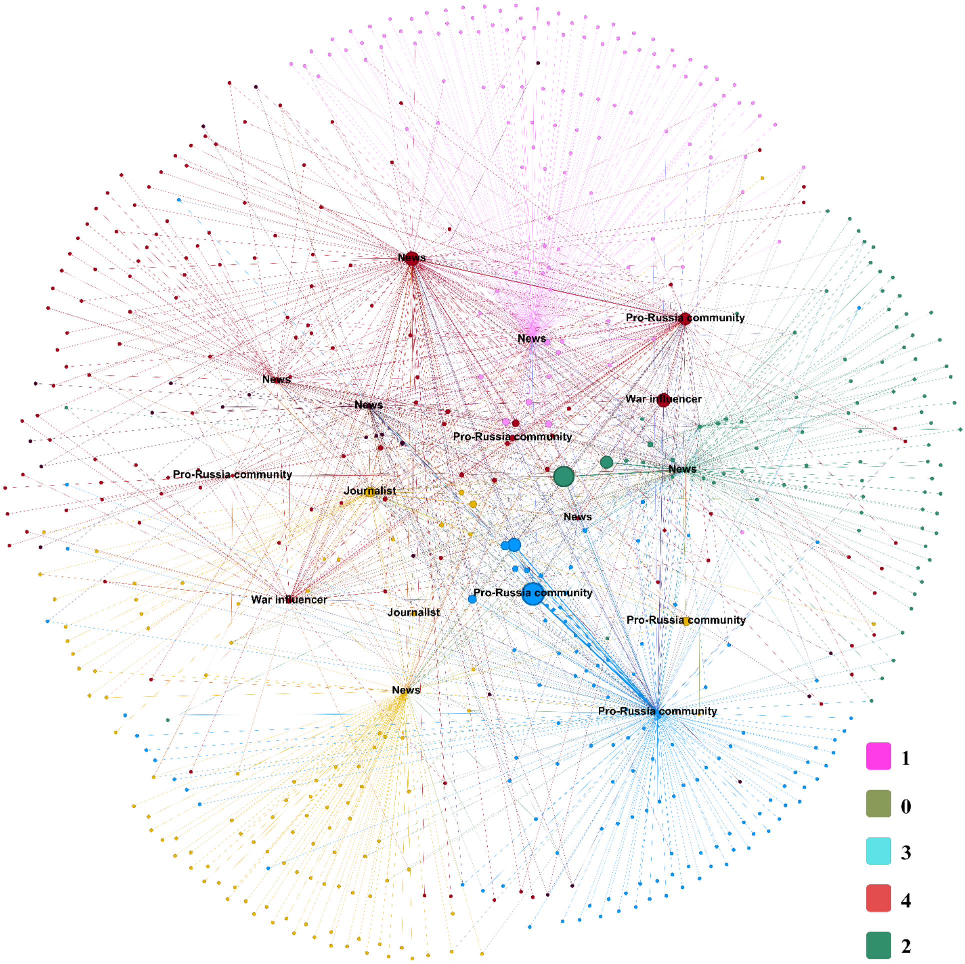


Source: own elaboration.

Fig. 2. Community layout of the Italian pro-Russia digital ecosystem on Telegram

Node level analysis

At a node level, two different measures have been considered. The first metric is degree centrality, which quantifies the number of nodes adjacent to a given node[34]. Specifically, in cases where direct data is available, the number of relations emanating from a node to other nodes is referred to as outdegree, while the number of relations directed towards the node from other nodes is referred to as indegree. It is important to note that a high degree centrality score does not necessarily imply leadership status, but rather indicates that the node under consideration has a large number of direct connections with other nodes.

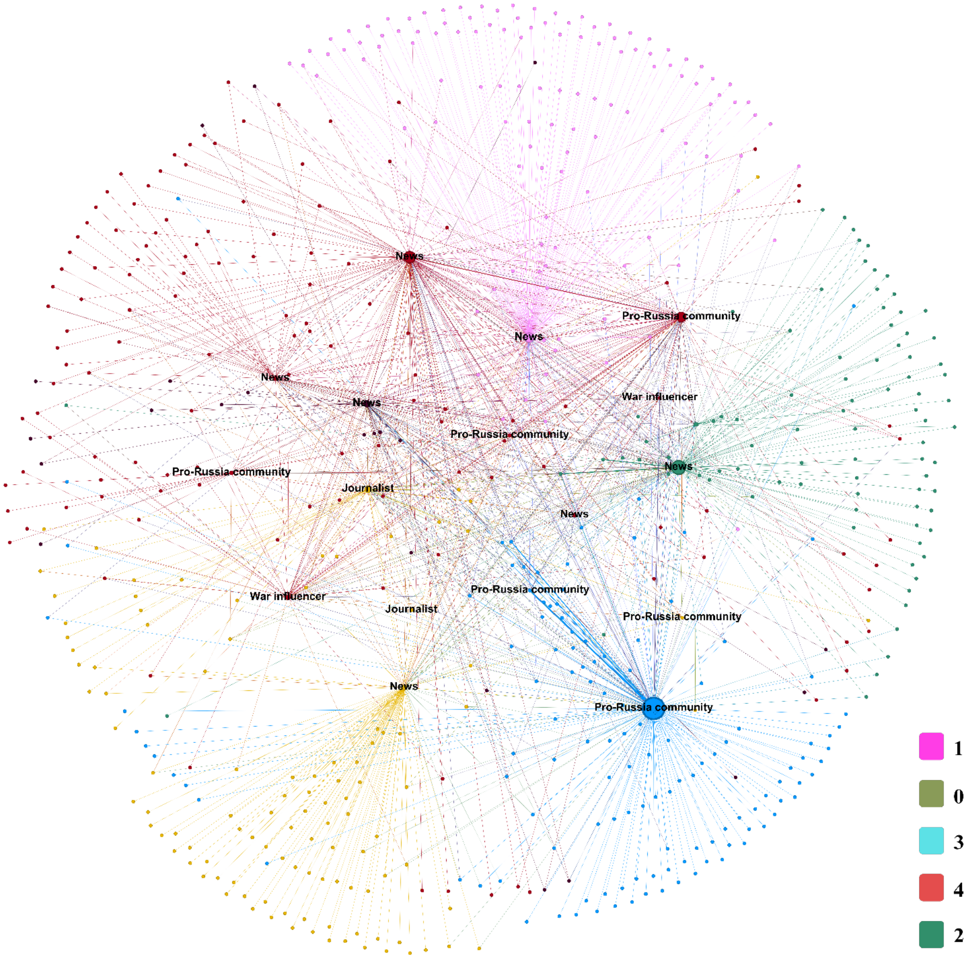


Source: own elaboration.

Fig. 3. Community layout with weighted outdegree of the Italian pro-Russia digital ecosystem on Telegram

[34] L.C. Freeman, D. Roeder, R.R. Mulholland, *Centrality in social networks: ii. experimental results*, „Social Networks" 1979, no. 2, p. 119–141.

The key nodes that serve as content producers were identified in Figure 3 through a weighted outdegree, representing the nodes that function as the primary news sources and those that flood the infosphere with pro-Russia narratives and disinformation propaganda. Within these channels, it is possible to identify the root pro-Russia communities and channels that disseminate information about the Russian government and the Russian-Ukrainian war.



Source: own elaboration.

Fig. 4. Community layout with weighted indegree of the Italian pro-Russia digital ecosystem on Telegram

On the other side, the nodes that receive and disseminate the most material were identified in Figure 4 using the weighted indegree measure. Such nodes contribute to a loosely-knit propaganda and disinformation network, which relies on feeble ties. Within these channels, it is possible to observe similar key nodes to those identified in Figure 3. Notably, it is observed that certain channels play a dual role in this network, by producing a significant amount of content that is shared by other nodes while simultaneously serving as a connector for different nodes. Considering these findings, it can be surmised that these key nodes play a crucial role in shaping the dynamics of the wider propaganda and disinformation network.

The betweenness centrality is the second examined metric to identify key nodes in the network. This measure quantifies the number of times a node is on the geodesic path between any two other nodes[35]. A high betweenness centrality score indicates a node that has the ability to connect channels that would otherwise not be directly connected. Therefore, a node in a brokerage position may not have many direct contacts, but its contacts are essential in linking different channels in the network. In this network, nodes with high betweenness centrality scores are primarily pro-Russia channels that disseminate news related to the Russian government and the Ukrainian conflict.

Conclusion

The use of social media for spreading disinformation and propaganda is becoming a major concern for policymakers and researchers alike, particularly in the context of geopolitical conflicts. The emergences of pro-Russia Telegram channels operating at a global scale, including in the Italian ecosystem, has highlighted the need for a deeper understanding of the dynamics of this platform and its role in disseminating disinformation. Telegram's loose content moderation policies have made it an ideal platform even for disinformation, as it is emerging in the context of the Russian-Ukrainian conflict.

This social network analysis of the Italian pro-Russia Telegram channels reveals a strong connection between channels closely linked to „official" Russia propaganda and those run by Italian news outlets, journalists, and war influencers. Russian propaganda seems to operate like a supply chain, where different actors play a crucial role in spreading the pro-Russia narrative in the cognitive warfare battlefields. Even proxy forces such as PMC Wagner

[35] Ibidem, p. 119–141.

are deployed in the cognitive warfare battlefield, actively disseminating information through pro-Russia Telegram channels. In particular, these channels heavily feature news and updates about PMC Wagner, making their activities a main topic within the network. Certain channels even provide subtitles of the interviews and official materials related to the group in Italian, while others make use of memes and songs to reinforce the pro-violence narrative and feed the fascination of PMC Wagner. Through their various tactics, these channels act as a window into the battlefield, simplifying the recruitment process and reinforcing the pro-Russia narrative. The influence of Russian propaganda on the Italian public opinion can have significant implications for Italian foreign policy towards Russia. Thus, the study of the dynamics of pro-Russia Telegram channels in Italy is a critical area of research that can shed light on the role of social media in spreading disinformation and propaganda in global conflicts.

In conclusion, this study demonstrates the capacity of social network analysis to extract significant insights from digital networks that can be utilized to draw valuable information on cognitive warfare. Through this analysis, it has been established that Russian disinformation permeates daily and is disseminated extensively within the Italian context, propagating a subversive sentiment that favours Russian interests. The results obtained through the application of social network analysis reinforce the importance of understanding the network structure of digital platforms in gaining a comprehensive insight into the cognitive warfare battlefront. Ultimately, it is proposed that through social network analysis techniques is possible to unveil the intricate groups that disseminate disinformation and influence the public opinion in the interest of foreign powers.

In consideration of this, future research should explore the sentiment of the content disseminated through these channels, as well as analysing mentions, in addition to forwards. Moreover, while this study exclusively focuses on the analysis of channels, future research should expand the analysis to include chats in order to identify key individuals, in addition to groups, and to achieve a more in-depth understanding of the actors involved in the dissemination of pro-Russia propaganda in Italy.

Bibliography

Aieva I., Moffitt J.D., Carley K.M., *How disinformation operations against Russian opposition leader Alexei Navalny influence the international audience on Twitter*, „Social Network Analysis and Mining" 2022, vol. 12, no. 1.

Arif A., Stewart L.G., Starbird K., *Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse*, „Proceedings of the ACM on Human-Computer Interaction" 2018, vol. 2.

Atkinson R., Flint J., *Accessing hidden and hard-to-reach populations: Snowball research strategies*, „Social Research Update" 2021, vol. 33, no. 1.

Badawy A., Ferrara E., Lerman K., *Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign* [in:] *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Lyon 2018.

Baltar F., Brunet I., *Social research 2.0: Virtual snowball sampling method using Facebook*, „Internet Research" 2012, vol. 22, no. 1.

Bastian M., Heymann S., Jacomy M., *Gephi: An Open Source Software for Exploring and Manipulating Networks*, „Proceedings of the International AAAI Conference on Web and Social Media" 2009, vol. 3, no. 1.

Blondel V.D., Guillaume J.L., Lambiotte R., Lefebvre E., *Fast unfolding of communities in large networks*, „Journal of Statistical Mechanics: Theory and Experiment" 2008, no. 10.

Bucher T., Helmond A., *The Affordances of Social Media Platforms* [in:] *The SAGE Handbook of Social Media*, eds. J. Burgess, A. Marwick, T. Poell, Thousand Oaks 2018.

Can U., Alatas B., *A new direction in social network analysis: Online social network analysis problems and applications*, „Physica A: Statistical Mechanics and Its Applications" 2019, vol. 535 (C).

Cao K. et al., *Countering cognitive warfare: Awareness and resilience*, NATO Review, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [access: 20.05.2021].

Cinciripini L., Borgonovo F., Zaliani M., *Propaganda weaponisation: Lo sfruttamento della pandemia da parte di attori non statali*, „Call for Papers #CASD 2020", no. 1.

Claverie B., Du Cluzel F., *Cognitive Warfare: The Advent of the Concept of „Cognitics" in the Field of Warfare* [in:] *Cognitive Warfare: The Future of Cognitive Dominance*, eds. B. Claverie, B. Prébot, N. Buchler, F. du Cluzel, Paris 2022.

Doroshenko L., Lukito J., *Trollfare: Russia's disinformation campaign during military conflict in Ukraine*, „International Journal of Communication" 2021, no. 15.

Dosek T., *Snowball Sampling and Facebook: How Social Media Can Help Access Hard-to-Reach Populations*, „PS: Political Science & Politics" 2021, vol. 54, no. 4.

Dutta U. et al., *Analyzing Twitter Users' Behavior Before and After Contact by the Russia's Internet Research Agency*, „Proceedings of the ACM on Human-Computer Interaction" 2021, no. 5 (CSCW1).

Eady G. et al., *Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior*, „Nature Communications" 2023, vol. 14, no. 1.

Etikan I., *Comparision of Snowball Sampling and Sequential Sampling Technique*, „Biometrics & Biostatistics International Journal" 2016, vol. 3, no. 1.

Ferrara E., *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election*, https://doi.org/10.48550/ARXIV.1707.00086 [access: 26.04.2023].

Freeman L.C., Roeder D., Mulholland R.R., *Centrality in social networks: ii. experimental results*, „Social Networks" 1979, no. 2.

Froio C., Ganesh B., *The transnationalisation of far right discourse on Twitter: Issues and actors that cross borders in Western European democracies*, „European Societies" 2019, vol. 24, no. 4.

Garcia A.C., Standlee A.I., Bechkoff J., Cui Y., *Ethnographic Approaches to the Internet and Computer-Mediated Communication*, „Journal of Contemporary Ethnography" 2009, vol. 38, no. 1.

Golovchenko Y., *Measuring the scope of pro-Kremlin disinformation on Twitter*, „Humanities and Social Sciences Communications" 2020, vol. 7, no. 1.

Golovchenko Y., Hartmann M., Adler-Nissen R., *State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation*, „International Affairs" 2018, vol. 94, no. 5.

Goodman L.A., *Snowball Sampling*, „The Annals of Mathematical Statistics" 1961, vol. 32, no. 1.

Grčar M., Cherepnalkoski D., Mozetič I., Kralj Novak P., *Stance and influence of Twitter users regarding the Brexit referendum*, „Computational Social Networks" 2017, vol. 4, no. 1.

Guess A.M., Nyhan B., Reifler J., *Exposure to untrustworthy websites in the 2016 US election*, „Nature Human Behaviour" 2020, vol. 4, no. 5.

Hung T.C., Hung T.W., *How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars*, „Journal of Global Security Studies" 2022, vol. 7, no. 4.

Klein O., Muis J., *Online discontent: Comparing Western European far-right groups on Facebook*, „European Societies" 2019, vol. 21, no. 4.

Knoke D., Yang S., *In Social network analysis*, 3 ed., Thousand Oaks 2019.

Krona M., *Mediating Islamic State\textbar Collaborative Media Practices and Interconnected Digital Strategies of Islamic State (IS) and Pro-IS Supporter Networks on Telegram*, „International Journal of Communication" 2020, no. 14.

Liadze I., Macchiarelli C., Mortimer-Lee P., Juanino P.S., *The economic costs of the Russia-Ukraine conflict*, London 2022.

Luceri L., Giordano S., Ferrara E., *Detecting Troll Behavior via Inverse Reinforcement Learning: A Case Study of Russian Trolls in the 2016 US Election*, „Proceedings of the International AAAI Conference on Web and Social Media" 2020, no. 14.

Morselli C., Giguère C., Petit K., *The efficiency/security trade-off in criminal networks*, „Social Networks" 2007, vol. 29, no. 1.

O'Callaghan D. et al., *An Analysis of Interactions within and between Extreme Right Communities in Social Media* [in:] *Ubiquitous Social Media Analysis*, eds. M. Atzmueller, A. Chin, D. Helic, A. Hotho, Berlin; Heidelberg 2013.

Ottewer P., *Defining the Cognitive Domain*, https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/ [access: 7.12.2020].

Owen T., *How Telegram Became White Nationalists' Go-To Messaging Platform. In Vice*, https://www.vice.com/en/article/59nk3a/how-telegram-became-white-nationalists-go-to-messaging-platform [access: 24.04.2023].

Paul K., Waterson J., *Facebook bans Alex Jones, Milo Yiannopoulos and other far-right figures*. „The Guardian", https://www.theguardian.com/technology/2019/may/02/facebook-ban-alex-jones-milo-yiannopoulos [access: 2.05.2019].

Postill J., Pink S., *Social Media Ethnography: The Digital Researcher in a Messy Web*, „Media International Australia" 2012, no. 1.

Rogers R., *Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media*, „European Journal of Communication" 2020, vol. 35, no. 3.

Sanovich S., Woolley S., Howard P., *Computational propaganda in Russia: The origins of digital misinformation*, „Working Paper" 2017, no. 3.

Situation in Ukraine, Security Council, 7683th meeting, https://www.unmultimedia.org/avlibrary/asset/1613/1613953/ [access: 28.04.2016].

Sloane W., *Putin cracks down on media*, „British Journalism Review" 2022, vol. 33, no. 3.

Ukraine Refugee Situation, https://data.unhcr.org/en/situations/ukraine [access: 22.03.2023].

Urman A., Katz S., *What they do in the shadows: Examining the far-right networks on Telegram*, „Information, Communication & Society" 2022, vol. 25, no. 7.

Wilson J., *Gab: Alt-right's social media alternative attracts users banned from Twitter*, „The Guardian", https://www.theguardian.com/media/2016/nov/17/gab-alt-right-social-media-twitter [access: 17.11.2016].

Yablokov I., *Russian disinformation finds fertile ground in the West*, „Nature Human Behaviour" 2022, vol. 6, no. 6.

Włoski prorosyjski cyfrowy ekosystem w Telegramie

Streszczenie

Rozpowszechnianie prorosyjskiej ideologii i związanych z nią motywów wizualnych stało się zjawiskiem powszechnym, obejmującym różne społeczności w ramach cyfrowego ekosystemu. Tendencja ta powiązana jest z tzw. wojną kognitywną, której celem jest manipulacja opinią publiczną, informacjami i podważanie wiarygodności instytucji demokratycznych. Jeśli chodzi o kontekst włoski, to w latach 2019–2023 nastąpił wyraźny wzrost liczby podmiotów promujących prorosyjską narrację. Do podmiotów tych można zaliczyć członków ruchów *no-vax* i *no-greenpass*, teoretyków spisku, organizacje skrajnie prawicowe, grupy neonazistowskie. Jednocześnie ekosystem cyfrowy przyczynił się do rozprzestrzeniania w internecie treści zawierających przemoc i propagandę skierowaną przeciwko establishmentowi. W celu zidentyfikowania i zbadania włoskiego ekosystemu cyfrowego dotkniętego prorosyjskimi ideologiami w badaniu wykorzystano analizy sieci społecznościowych w usłudze komunikatora Telegram. Dzięki takiemu podejściu badanie to zapewniło wgląd w strukturę organizacyjną i dynamikę sieci, identyfikując kluczowe podmioty i ich relacje oraz wzorce rozpowszechniania prorosyjskiej propagandy. Niniejszy artykuł proponuje także nową metodologię badawczą do badania ekosystemów cyfrowych przesiąkniętych kampaniami wojny kognitywnej, zapewniającą głębsze zrozumienia mechanizmów, za których pomocą takie treści są propagowane, umożliwiającą opracowanie skutecznych strategii przeciwdziałania dezinformacji i promowania dyskursu opartego na faktach.

Słowa kluczowe: Rosja, dezinformacja, wojna poznawcza, Włochy, analiza sieci społecznościowych