

UDC 930.2: 004+32.019.57: 355.48(477:470)"2014/2022"
DOI <https://doi.org/10.32782/2663-5984.2025/2.39>

Shyshkina Ye. K.

National Technical University "Kharkiv Polytechnic Institute"

INFORMATION TECHNOLOGIES IN POLITICAL PROPAGANDA: THE CASE OF THE RUSSIAN-UKRAINIAN INFORMATION WAR (2014–2022)

The article analyzes the shift in 2014 of the Russian Federation to the policy of covert military intervention in Ukraine, which was accompanied by the strengthening of information influence. It was exerted both on the population of Russia, as it was increasingly seen as a mobilization resource, and in the former Soviet republics, primarily Ukraine. The publication argues that during this period a digital propaganda system was made purposefully and with the involvement of significant and versatile resources. It was extremely similar to the classical model typical for totalitarian society, as it performed the same functions in the virtual world: "digital censorship and repressions" ("trolling"), "digital iron curtain" ("filter bubble"), etc. The model of creation and behavior of such a digital propaganda system was reconstructed. The author calls the most successful tool a combination of methods of influence: creation of a large sector of Russian-language propaganda content on the Internet; filling it with propaganda templates, Russian "newspeak" phrases, fakes in order to reduce attention; opening "trolling farms" that perform the function of moderating "public opinion", implementing "digital censorship" and "repression", as well as sending messages with links to propaganda content; artificially drawing people through the effect of a "filtering bubble" into the bubble with propaganda information, isolating the user through this effect from other sources of information (i.e., creating a "digital iron curtain"); using people who were influenced to further broadcast propaganda templates offline. Russian-language content was identified as the main limitation of this method, and increased visualization of propaganda to attract young people was predicted.

Key words: information war; computer science, information technology, propaganda, computing technology, history of science and technology, multidisciplinary, digital sources, methodology of history.

Statement of the problem. The intensification of international confrontation in the world, the shift to "hard power" in political communication, the intensification of the use of computer technologies in all spheres of life of the population actualize the interest of society and specialists to the issues related to the use of the latest information tools in the process of manipulating mass consciousness.

Recent events in Russia and Ukraine (primarily Crimea and Donbass) confirm the implementation in practice of a number of the latest methods of influence, based, on the one hand, on the rich historical experience in the sphere of propaganda activities typical for totalitarian regimes (especially the USSR), and, on the other hand, on the use of the latest technologies. In form, they are digital; in substance, they are borrowed often from developed countries and other areas (methods of attracting customers, clients, voters, new members of religious sects, etc.).

Analysis of recent research and publications. Today, there is a large group of studies that examine

the use of information technologies in historical retrospect and within the criticism of historical sources; publications that explore the peculiarities of propaganda work in history; as well as researches on the Russian-Ukrainian practice of information confrontation at the present stage.

The first group of studies has accumulated valuable experience of computer methods application in historical science (Aspray W. 2024 [1], Burns W. 2020 [2], etc.). They review the history of the use of information technologies and show the methodological features of information analysis, thus making it possible to find a balance in the process of combining traditional historical approaches with new computer tools for collecting and analyzing information.

The second group of publications is useful for highlighting the main features and basic tools of propaganda based on data from different spatial and temporal frameworks (Henschke A. 2024 [3], Akande A. 2023 [4], etc.). These publications present

the history of propaganda methods, use specific historical examples to identify the peculiarities of their implementation, show their effectiveness in achieving certain goals, and demonstrate the consequences of the use of such methods.

Finally, the last group of studies helps to make an overall picture of the peculiarities of Russia's information aggression against Ukraine at the present stage. Many historical papers in this group of research focus on the issues of instrumentalization and falsification of history (Weiss-Wendt A. 2022 [5], Yakubova L. 2023 [6]). Other studies focus on the role of mass media in the process of dissemination of political propaganda (Danilian O., Dzioban O. 2022 [7], Sinchak B. 2022 [8]).

When discussing the problems of information security, more often it is raised the problems of fraud and cyber-attacks, to a lesser extent the issue of propaganda dissemination in Internet and social networks is studied (Zalevskaya, I., Udrenas, G. 2022 [9], Petrenko S., Nazarenko N. 2024 [10]).

As for the reconstruction of a model of the information system as a comprehensive tool of influence, such studies, unfortunately, have not been conducted, although they are essential in the current situation.

Task statement. The aim of the article is to reconstruct the mechanism of dissemination of Russian propaganda and its impact on the public based not only on the data from the historical experience of propaganda use in totalitarian societies, but also on information technologies and the latest methods of attracting new supporters in the course of the information war of 2014–2022.

To achieve this goal, both traditional methods for historical science and techniques of digital data analysis will be used. The principle of objectivity will be realized by focusing on the public component of the problem, since the chronological framework of the study corresponds to recent times, and only open sources are available for study.

The research methodology will be based on the use of quantitative data and qualitative research of digital sources. It will be based on the traditional methods of heuristics, external and internal criticism. However, they will be supplemented with digital tools.

The source base of the research will include materials from official websites of organizations involved in the information struggle, collections of bot messages, fakes, trolling postings, and statistical data.

Outline of the main material of the study. 2014 was a landmark year in the sense that it reoriented

Russia to prioritize tools for territorial expansion. Although the Russian Federation still tried to maintain the look of “soft power”, it had to constantly expand the range of tools for information influence, gradually moving to “hard power”.

The situation in the information field from 2014 to 2022 is characterized by a number of specific features, which are proposed to be grouped as follows.

The first and most important aspect of the Russkiy Mir in this period is the linguistic one. Since 2014, support for the Russian language has become more active and manifested itself in the creation of *extensive Russian-language content* on the Internet and social networks. Analysis of statistical data gathered by World Wide Web Technology Surveys allows us to say that in the period from 2014 to 2021, the share of Russian content doubled, and at the beginning of the full-scale invasion of Ukraine, it ranked in second position after English-language [11].

The second aspect is the use of *Russian newspeak*. To create a public sphere different from the real one, Russia actively used euphemisms. The substitution of notions has become a common practice in Russian politics both within the country and in the international arena. In Ukraine, Russian newspeak has become an integral part of Russian information aggression. It became a widespread Russian media trend since V. Putin's speeches of 2014.

The third tool is the use of “bots” and “trolls”. “Bots” were used to disperse propaganda material across the networks. They also created the impression of mass support by “public opinion” for certain patterns of Russian propaganda, aimed at forming the illusion of a positive attitude toward the Russkiy Mir, etc. “Troll factories” motivated discussions and moderated “public opinion” by positively evaluating certain messages and aggressively criticizing undesirable opinions, exercising “digital censorship” and “repression” [12].

According to the results of the research made by VoxUkraine, which analyzed trolling on Twitter (it should be said that this is only a very small segment of activity, since Twitter is not the most popular network in Ukraine and Russia), the first peaks of troll activity were on dates related to the annexation of Crimea, the so called “referendum” there, and the presidential election in Ukraine. It reached the highest point on July 17, 2014, at the time of the shooting down of the civilian passenger plane of Malaysia Airlines.

It is difficult to assess “troll factories” today, since such organizations are hidden. It is known from open sources that the largest organization engaged in such activities in Russia was the Internet Research Agency,

created in 2013. A few journalistic investigations indicate that Ukraine was far behind the Russian side in the scale and quality of “trolling”; moreover, there is no evidence of its use to provide resistance in the information war (Table 1) [13].

As for the Russian information field, it was only with the beginning of the large-scale invasion of Ukraine that a “legion of elves” was created based on the Russian opposition organization Free Russia Foundation, which, however, cannot organize much resistance. According to research of Russia’s most popular network Vkontakte, made by Re: Russia. Expertise, Analysis and Policy Network, the messages of the “legion of elves” account for only 11% of all bot messages. While “evil Kremlebots” (which carry out propaganda of aggression against Ukraine) and “good Kremlebots” (which positively assess Russia’s development and hide aggression behind peace goals) make up 79% of all bot messages [14].

The fourth aspect is *fakes*. The widespread dissemination of fakes since 2014 has led to the need to create special organizations to combat Russian fakes, not only in Ukraine but also in a number of other countries [15].

The fakes fulfilled a double function. For those who were ready to believe in them, they were an aid in the process of propaganda influence. For those to whom the ridiculousness of the fakes was obvious, they helped to create an atmosphere of “chaos” and distrust of all sources of information, including truthful ones.

Thus, a significant part of the population simply stopped asking questions about the truth and relying on rational arguments and began to take everything on faith. The “information noise” allowed to transfer of a significant part of the people from the sphere of rational to the sphere of emotional, from conscious to subconscious, as a result, it became easier to carry out propaganda influence.

The influence of Russian “bots” and “fakes”, however, worked effectively within the Russian

Federation, but to a lesser extent on the Ukrainian population. So, to strengthen propaganda, the fifth aspect – the “*filter bubble*” – was used. Its effect was described most fully in the works of Pariser Eli [16].

A problem resulted from the use of individualized information selection by search systems. The effect was no new but Russia utilized it massively in politics.

Since the machine determines “interests” by the frequency of going to certain sites, stimulating people to follow certain links in various ways, it became possible to artificially immerse them in content that promotes the Russkiy Mir and exert a long-term influence on the subconscious by creating a digital isolation that prevents people from leaving “bubble”.

The analyses of the mechanism of influence allows us to distinguish such components of the process. The first step is creating a message for social media. It should have the following characteristics:

- 1) the emotionally saturated, useful, and relevant information for the population;
- 2) the connection of the message with a propaganda template or “Russian newspeak”;
- 3) the presence of a link to a site with propaganda content.

At the next stage, “bots” and “trolls” spread such messages on social networks. Since they carry an emotional, useful, and relevant load, their further dispersal is ensured by unsuspecting citizens.

Each recipient of such a message, by opening a link, makes the system think that such content is the user’s “interest”, and the “filter bubble” effect immerses him/her in a bubble with propaganda content. In this way, an authoritarian/totalitarian political regime creates a digital “iron curtain”, first around the individual, then around his family, friends, and finally around millions of people (this explains the rapid spread of propaganda in the Russian Federation).

The main limitation of this method is the predominantly Russian-language content. Seeing these boundaries, the Russian intellectual elite began

Table 1

Comparison of the trolling of the Internet Research Agency (Russia) and Pragmatico (Ukraine)

RUSSIA (INTERNET RESEARCH AGENCY)	UKRAINE (PRAGMATICO)
foreign policy	local customers
all kinds of social networks Russian-language “VKontakte”, international Facebook, Twitter, Instagram, and YouTube	mainly Facebook
the norm is 135 comments per day	the norm is 300 comments per day
300–400 people	20 people
interests of the Kremlin	interests of individual politicians

Table is made by author on data from “Deutsche Welle”

to look for ways to expand the influence of the Russkiy Mir beyond these borders.

Among alternatives was the financing of propaganda media in other languages. Investments in the most important Russian media abroad sometimes significantly exceeded investments in the key media of the state, which acted as an object of propaganda influence (see the report for Friedrich-Naumann-Stiftung für die Freiheit about “Russia today” and “Deutsche Welle” in 2014–2022 [17]). But even more effective is seen the use of visual propaganda (computer games, promotional and concept art, futuristic and “historical” 3d visual projects, etc.), which has not acquired mass use in 2014–2022, but will obviously become the main focus shortly, as it is oriented to the younger generation.

Conclusions. Thus, in 2014, Russia shifted to a policy of covert military expansion. The main object of its influence was, on the one hand, its own population, which was more than before regarded as a mobilization resource for warfare, and therefore required more extensive ideological processing. On the other hand, the Russian-speaking population of the former Soviet republics, especially Ukraine. Information efforts were aimed at splitting the country and stimulating civil confrontation.

To this end, the latest advances in digital information technologies were used. The most successful of

them, in our opinion, was the combination of several methods of influence:

1) creation of a large sector of Russian-language propagandistic content on the Internet, involving scientists from different fields, including historians, in the preparation of such content,

3) filling it with propagandistic templates, phrases of “newspeak”, fakes to reduce attention (a common method of attracting new members in religious sects), i.e., taking people out of the “rational”, transferring “consciousness” into the “subconscious”,

3) opening “trolling farms” that perform the function of moderating “public opinion”, implementation of “digital censorship” and “repression”, as well as sending messages with links to propaganda content,

4) artificially drawing people through the effect of a “filter bubble” into the bubble with propaganda information, the isolation of the user due to this effect from other sources of information (i.e., the creation of a “digital iron curtain”),

5) using people who have been influenced to further broadcast propaganda templates to their relatives, friends, and acquaintances offline.

The main limitation of this method was Russian-language content. Other approaches (e.g., the use of visuals) were considered, but were not prioritized during the researched period.

Bibliography:

1. Aspray, William *Writing Computer and Information History: Approaches, Connections, and Reflections*. Rowman & Littlefield Publishers, 2024. 425 p.
2. *Science and Technology in World History* / Burns William E. (ed.). ABC-CLIO, 2020. 893 p.
3. Henschke, Adam *Cognitive Warfare: Grey Matters in Contemporary Political Conflict*. Routledge, 2024. 276 p.
4. Akande, Adebawale *Handbook of Racism, Xenophobia, and Populism: All Forms of Discrimination in the United States and Around the Globe*. Springer, 2023. 1003 p.
5. Weiss-Wendt, Anton *Putin's Russia and the Falsification of History: Reasserting Control over the Past*. Bloomsbury Academic, 2022. 338 p.
6. Якубова, Лариса *Російсько-українські «історичні війни»: введення в дискурс ненависті і знищення. Аналітична записка* / Відповідальний редактор В.А. Смолій. Київ: Інститут історії України НАН України, 2023. 68 с.
7. Данильян, О. Дзьобань, О. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2022. № 3 (54). С.11–29.
8. Синчак, Богдан *Прямоефірна інформаційна війна та російсько-українська війна 2022-го на медійному плацдармі. Український інформаційний простір*. 2022. № 2 (10). С. 85–97.
9. Залєвська, І.І., Удренас, Г.І. Інформаційна безпека України в умовах російської військової агресії. *Південно-український правничий часопис*. 2022. № 1–2. С. 20–26.
10. Петренко, Світлана; Назаренко, Наталія *Інформаційна гігієна як засіб протидії інформаційним впливам у контексті російсько-української війни. Інформаційна безпека людини, суспільства, держави*. 2024. № 1–3 (34–36). С. 30–38.
11. Historical Trends in the Usage of the Top Content Languages 2013–2024: *World Wide Web Technology Surveys*. URL: https://w3techs.com/technologies/history_overview/content_language/ms/y
12. Колекція бот-повідомлень. URL: <https://botnadzor.org>

13. Беляева Яна «Фабрики троллей» – новый стандарт в политическом пиаре? *Deutsche Welle*. December 14, 2019. URL: <https://surl.lu/poqnkn>
14. Sokolova Alesya Bots in contact: how online propaganda works. *Re-Russia: expertise, analysis and policy network*, May 07, 2024. URL: <https://re-russia.net/en/expertise/0147/>
15. Orlova, Daria; Makar, Olga; Romaniuk, Viktoria; Zhdanova, Maria Fakes Debunked by the StopFake Project between 2014–2017: Narratives and Sources. Stopfake: official website. September 20, 2018. URL: <https://surl.lt/tenukx>
16. Pariser Eli: *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Books, 2012. 294 p.
17. Spahn Susanne *Russian Mass Media in Germany. How Russian information war and disinformation are affecting Germany*. Potsdam-Babelsberg: Friedrich-Naumann-Stiftung für die Freiheit, 2020. 27 p. URL: <https://www.freiheit.org/east-and-southeast-europe/russian-media-germany>

Шишкіна Є. К. ІТ-ТЕХНОЛОГІЇ В ПОЛІТИЧНІЙ ПРОПАГАНДІ НА ПРИКЛАДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ (2014–2022 РР.)

У статті аналізується перехід у 2014 році Російської Федерації до політики прихованого військового втручання в Україну, що супроводжувалося посиленням інформаційного впливу. Воно поширювалося як на населення Росії, яке дедалі більше розглядалося як мобілізаційний ресурс, так і на території колишніх радянських республік, насамперед України. У публікації стверджується, що в цей період цілеспрямовано та із залученням значних і різнобічних ресурсів створювалася система цифрової пропаганди, яка була надзвичайно схожа на класичну модель притаманну тоталітарному суспільству, оскільки виконувала ті самі функції у віртуальному світі: «цифрова цензура та репресії» (через «тролінг»), «цифрова залізна завіса» (через «пузир фільтрів») тощо. Реконструйовано модель формування та поведінки такої системи цифрової пропаганди. Найбільш вдалими інструментами автор називає поєднання кількох методів впливу: створення великого сектору російськомовного пропагандистського контенту в Інтернеті, наповнення його пропагандистськими шаблонами, «новоязівськими» фразами, фейками з метою зниження уваги, відкриття «тролінгових ферм», які виконують функцію модерації «громадської думки», впровадження «цифрової цензури» та «репресій», розсилка повідомлень із посиланнями на пропагандистський контент, штучне втягування людей через ефект «пузиря фільтрів» в бульбашку з пропагандистською інформацією, ізоляція користувача через цей ефект від інших джерел інформації (тобто створення «цифрової залізної завіси»), використання людей, які зазнали впливу, для подальшого транслявання пропагандистських шаблонів офлайн. Основним обмеженням цього методу було визначено російськомовний контент і спрогнозовано посилення візуалізації пропаганди для залучення молоді.

Ключові слова: інформаційна війна, інформатика, інформаційні технології, пропаганда, обчислювальна техніка, історія науки і техніки, мультидисциплінарність, цифрові джерела, методологія історії.