Journal of Siberian Federal University. Humanities & Social Sciences
2022 15(12): 1738–1750

DOI: DOI: 10.17516/1997-1370-0948
EDN: IGVUQA
УДК 316.4; 004.891

An Online Scan of Extreme-Right Radicalization in Social Networks (The Case of the Russian Social Network VKontakte)

Anna Yu. Karpova*, Sergey A. Kuznetsov, Aleksei O. Savelev and Alexander D. Vilnin
National Research Tomsk Polytechnic University
Tomsk, Russian Federation

Received 17.06.2021, received in revised form 11.12.2021, accepted 19.04.2022

Abstract. The aim of the research is to develop software prototypes for studying the mechanisms of extreme right online radicalization via using the Web Mining and AI methods. We consider online radicalization as a process of transition from non-violent forms of expressing opinion online to committing violent acts offline. Online forums are becoming a "course-book" on toxic behavior and provide a cyber transition from traditional moderate political discourse to the radical rhetoric of the "hate speech". To search targeted online communities we designed and implemented a unique algorithm for calendar-correlation analysis (CCA) of online community activity. The algorithm was tested on data from the Russian social network VKontakte. The CCA algorithm can be used as an additional tool for automated assessment of membership in extreme right ideology if having an appropriate knowledge base. We identified factors that significantly influence the efficiency of research automation on the online radicalization study.

Keywords: radicalization, extremism, extreme right, web mining, computational social science.

This research was carried out within the state assignment of the Ministry of Science and Higher Education of the Russian Federation as a part of the project No. FSWW 2020-0014.

Research area: law.

Citation: Karpova, A. Yu., Kuznetsov, S.A., Savelev, A.O. and Vilnin, A.D. (2022). An online scan of extreme-right radicalization in social networks (the case of the Russian social network VKontakte). J. Sib. Fed. Univ. Humanit. soc. sci., 15(12), 1738–1750. DOI: 10.17516/1997-1370-0948

* Corresponding author E-mail address: belts@tpu.ru

Онлайн-сканирование ультраправой радикализации в социальных сетях (на примере российской социальной сети «ВКонтакте»)

А.Ю. Карпова, С.А. Кузнецов, А.О. Савельев, А.Д. Вильнин
Национальный исследовательский Томский политехнический университет Российская Федерация, Томск

Аннотация. Целью исследования является разработка прототипов программных систем для изучения механизмов крайне правой онлайн-радикализации с использованием методов веб-майнинга и искусственного интеллекта. Мы рассматриваем онлайн-радикализацию как процесс перехода от ненасильственных форм выражения мнений в Интернете к совершению насильственных действий в автономном режиме. Онлайн-форумы становятся «учебным пособием» по токсичному поведению и обеспечивают киберпереход от традиционного умеренного политического дискурса к радикальной риторике «языка ненависти». Для поиска целевых онлайн-сообществ мы разработали и внедрили уникальный алгоритм календарно-корреляционного анализа (ККА) активности онлайн-сообщества. Алгоритм был протестирован на данных из российской социальной сети «ВКонтакте». Алгоритм ККА может быть использован в качестве дополнительного инструмента для автоматической оценки принадлежности к крайне правой идеологии при наличии соответствующей базы знаний. Мы выявили факторы, существенно влияющие на эффективность автоматизации исследований по изучению онлайн-радикализации.

Ключевые слова: радикализация, экстремизм, ультраправые, интеллектуальный анализ веб-данных, вычислительная социальная наука.

Исследование выполнено при финансовой поддержке ГЗ «Наука» в рамках проекта FSWW-2020-0014.

Научная специальность: 12.00.00 – юриспруденция.

Introduction

More than a hundred years have passed since the release of David W. Griffith's silent drama film "The Birth of a Nation (The Clansman)" in 1915 in America. Despite the fact that the film caused public outrage and mass protests calling to ban the film, a flurry of criticism in the press, the film had stood at the peak of popularity for almost all 20th century. With the advent of sound film, the movie received its "second birth," and the new versions of the soundtrack for the film created in the 21st century became a musical clue to identify supporters of extreme right ideology. The avowedly racist movie laid the foundation for an entire cinematic industry of promoting extreme right ideas and framed an art form of glorification of white supremacy supporters. The film influenced the Ku Klux Klan revival, the rise and promotion of the extreme right ideology as well as the reconstruction of political racism in the United States.

A hundred years later, a Christchurch mosque shooter (a terrorist attack in March

2019, New Zealand), a staunch extreme right supporter of the "white genocide" had demonstrated for 17 minutes to the world the unlimited possibilities of digital technologies to achieve his ideological goals. The gamification of massacres is not new. Jihadists widely used it in their media technologies, which were called by a British journalist Jason Burke as a "Selfie Jihad" (Burke, 2016). It was the incident where its live broadcasting was the application of jihadist "selfie jihad" tactics by extreme right terrorists. A Norwegian extreme right terrorist Breivik thought about the use of such tactics (terrorist attack in 2011). In the early stages of planning the attack, he intended to assassinate the former Norwegian Prime Minister, to film that on the smart phone and load it on the YouTube channel. The live broadcast of the Christchurch mosque massacre in popular social network Facebook, the publication of a racist manifesto, reports of a planned attack in the 8chan imageboard became an attractor for the extreme right in all parts of the planet and a universal hint for copycats. Thus, in 2019 the El Paso Walmart store shooter (Texas, USA) and the Poway synagogue shooter (California, USA) referred to the Christchurch shooter in their manifests posted on the Internet.

What is common in the technologies of 20th and 21st centuries? They demonstrate a certain milestone, a paradigm shift of the new technology for promoting violent extremism, terrorism on the ideological platform of the extreme right. The 20th century is the era of using a new technology of promotion extreme right ideology in cinematography. The 21st is the era of the Internet with countless ways of promotion extreme right ideology put into digital technologies. They are connected by the use of technical products, served as a key mechanism for the extreme right groups to use technological innovations for achieving ideological, political, economic and other goals. Unprecedented speed and density of communication are provided by improving communication channels, as well as by spreading social services. In January 2020 there were 4.54 billion Internet users in the world (59 % of the world population). And the number of active users of social media reached 3.8 billion (49 % of the world population) (Kemp, 2020).

Extreme right radicalization

The predictor of hate crimes, violent extremism, and terrorism is radicalization. In general terms, radicalization is thought of as a process of escalation from non-violent forms of opinion expression to more severe forms of violent behavior and readiness for violent actions. A criterion for the legal evaluation of the ultra-radical actors' and communities actions is the assessment of the risk level of their methods to society and the state, and whether it falls under existing legislation in different countries. The extreme right accept the idea that violence is necessary to achieve any goals: ideological, political, economic and even personal. They justify and sell this line, express a willingness to move on to violent actions, and also take a moral obligation to protect those groups that promote this idea.

In 2018, the *International Centre for the Study of Radicalisation* focuses in its report on the fact that in recent year's Islamic terrorism had absorbed the lion's share of the resources of law enforcement agencies and intelligence services, and this was true considering the degree of threat on the part of these organizations (ICSR, 2018). However, that was due to the reduction of investing the resources in other areas, meanwhile the extreme right groups were being developed and mobilized throughout Europe (Heide et al. 2018). This view is supported by researchers of ICCT (ICCT, 2021), START (START, 2021), C-REX (C-REX, 2019), academic scientists in sociology, psychology, history, criminology, and those who study terrorism (Wahlström et al., 2020; Colley and Moore, 2020).

In the 2020 annual report of the world's largest Munich International Security Conference experts stated that right-wing extremism is a key question on the agenda along with the space security, climate security and the technological race (Munich Security Report, 2020). According to the Institute for Economics & Peace:

- over the last 8 years people, motivated by radical right-wing ideology, have committed

almost three times more terrorist attacks than Islamists (Global terrorism index, 2020);

- the number of cases of extreme right terrorism is increasing, especially in Western Europe, North America and Oceania. The total number of incidents has increased by 320 % over the past 5 years (Global terrorism index, 2020);
- the three largest politically motivated terrorist incidents in the West for the last 50 years were perpetrated by the extreme right (Global terrorism index, 2019);
- the increasingly decentralized nature of both the global Islamist and extreme right-wing movements is largely due to the growth of the online extremist ecosystem (Global terrorism index, 2019; Gaudette et al., 2020; Poole et al., 2021);
- extremist groups flourish on crisis narratives, but digital analysis demonstrates how the ways of using pandemia for extremist purposes are changing and growing (Global terrorism index, 2020).

The activity of extreme right groups in Russia can only be partially described as systematic monitoring studies are not either carried out at all or are not published. There are no open publications of official statistics, systematic in-depth analysis of incidents. Many incidents often do not fall into the headlines or journalists rely on poor (unverified) sources in their publications, the circumstances of the incidents remain extremely vague. A potentially reliable source of information (although data are not complete) is an open database of the information and analytical center "Sova". According to official data over the last 10 years the number of hate crimes in Russia, that is, criminal crimes committed on the basis of ethnic, religious and similar enmity or prejudice has decreased while it is difficult to assess the true scale of what is happening. In 2019 the number of racist and neo-Nazi motivated attacks in Russia decreased though the number of murders was higher. Hate motivated incidents were registered in 18 regions of the Russian Federation in 2019, in 2018 – in 12 regions. Attacks on "ethnic strangers" remain the dominant category, and their number has increased compared to the previous year. The second group is crimes against political and ideological opponents. In 2019 the number of attacks on representatives of LGBT communities increased. The topic of doxxing by extreme right remained relevant. "Photos, personal data of anti-fascists, left-wing activists, independent journalists, law enforcement officials and threats against them appeared on the social networks web-pages of these organizations and groups (Yudina, 2019) According to the Levada Center data, in 2019 major mass ethnic unrest, an increase in xenophobic sentiment and incidents were noted against such an ethnic community as gypsies" (Levada Center, 2019).

In 2020 experts of the "Sova" center noted a burst of street activity in the form of rallies, protest actions, but also a continuing decrease in the number of participants in the Russian Marches since 2014. Moreover, experts remark that in recent years the proportion of activity in election campaigns remains steady high as it does not require great resources, and in comparison with rally activity, the main thing is that it does not face opposition from the authorities (Yudina, 2020).

Technological Context: opportunities and limitations

Despite the growth of radicalization research in recent years, empirical studies still represent only a small percentage of knowledge. It is partly due to the lack of a unified concept of radicalization, systematic studies are not possible to capture the complexity of the factors involved in the online radicalization process. We define online radicalization as the process of transition from nonviolent forms of expressing opinion online to doing violent actions offline. The quintessence of the process is a destructive information-psychological impact (DIPI) on social networks users in the online environment by applying information and communication technologies to achieve ideological, political, economic and other goals (Karpova et al., 2019; Karpova et al., 2020).

Counter-radicalization as a predictor of violent extremism and terrorism is currently being developed at three levels: the first level is to reduce the probability of the entire radicalization in population; the second level is

focused on identifying vulnerable categories of individuals for radicalization; the third level is focused on those who are already radicalized. The relevance of solving the problem of diagnosing and counteracting individual and group radicalization of young people in Russian social networks is determined by the need to quickly identify vulnerable categories of young people. Application of methods of intellectual analysis of web mining and artificial intelligence (AI) can potentially provide speed, reliability and efficiency of computer analytical methods and software system prototypes created on this basis. The adaptation of modern information technologies for the purposes of the subject area provides digital transformation for solution to sociological problems promptly and with a large data amount (Anderson, 2012). The efficiency of digital transformation directly depends on the organization of cooperation between data scientists, domain experts and professional service providers, who provide cloud repositories, digital platforms, application software, etc.) (Siebl, 2019).

Thus, today it is impossible to study the radicalization process to the full extent excluding the data that is publicly available in social networks. At the same time, there are factors that significantly influence the efficiency of automation of online radicalization research. We have conventionally classified them into three main levels, reflecting the sequence of data analysis:

1. Limitations of data extraction level. The main way to extract raw social media data is to work with Application Programming Interfaces (APIs), developed by social media owners via data provision methods. The rules for API use are set by the social media themselves, including the permissible frequency of requests, the amount of data provided in response to the request, etc. The use of several social media as primary data sources entails the development of a multi-agent acquisition subsystem. Apart from being a technically challenging task, especially for small research teams, it also means that we completely depend on social media owners.

2. Limitations of the level of data processing. Despite the extraordinary amount of data being publicly available in social media, it is still insufficient. There is no explicit information about the nature of the connections between users and communities. There is no possibility to verify the available information (as a consequence, it is impossible to evaluate the accuracy of models based on machine learning methods) (Tang and Liu, 2010). Thus, we are in the situation when we cannot ignore the available online information, as it is potentially able to improve the accuracy of the scientific worldview, but herewith we cannot base on the online data solely when make decision.

3. Limitations of the level of data interpretation. The development of artificial intelligence methods and their accompanying increases the qualification requirements to researchers. In this case, not just additional competence development programs and new educational trajectories are necessary but a qualitative formalization of already accumulated experience and knowledge that allows to transit to algorithm development.

Online extreme right radicalization: specifics

Social networks are a source of data for identifying ultra-radical actors/communities, for studying and predicting their behavior and actions. The relevance of identifying mechanisms of individual and group online radicalization in social networks is determined by the necessity to promptly prevent violent incidents of an extremist and terrorist nature. One of the most well-known aspects of social media is the ability to adapt the content, appeared in users' channels, addressing their specific values and interests, and insert in networks of their like-minded. This is what makes it a key asset for extremist and terrorist groups. Both in physical and virtual worlds such groups notedly rely on the isolation of potential recruits from views and opinions that diverge from their prevailing beliefs. Extreme right communities strive for including people in "echo chambers" that strengthen their messages and deject any opposing opinions. Thus, online communities by their nature create an environment, promoting radicalization for their users. The global, viral, scalable nature is what distinguishes on-

line radicalization from offline one. The use of social media by extreme right communities is rapidly developed and effectively adapted to the ever-changing opportunities of the online environment. Therein lies the challenge of studying online radicalization.

Online forums become a "course book" for toxic behavior in fact and provide a cyber transition between traditional moderate discourse and the radical rhetoric of "hate speech" (Holt et al., 2020; Daniels, 2009). For example, the creators of AIN (YouTube's alternative influence network) strive for providing an alternative source of information to the young disappointed media consumers, give a sense of countercultural rebellion, express distrust to "leading" news media, and frame the content as careless, interesting, rebellious and fun. Applying marketing techniques, instead of selling a product or service, they sell political ideology. Such sites make the audience radicalized by transmitting from mainstream to extremist content via guests' statements and crosslinks. Online discussion presenters themselves (academics, media experts, Internet celebrities) often move to more radical positions and subsequent interactions with other influential individuals in extreme right communities, promoting and actually advertising ideological radical beliefs. In general, AIN disseminates the extreme right content, using means of influence to purposefully create a common countercultural identity (Lewis, 2018).

The researchers, specialized in studying radicalization and technologies of promoting extreme right ideology, notice the tendencies which are necessary to be focused on:

- New communication technologies make possible and support the integration of extremists, mainstream and cross-platform coordination of the extreme right extremists.
- The issue of various forms of extreme right extremists' ideological organization stays relevant. Extreme right communities are branched out, "specializing" in problematic, urgent topics of public discontent, the large volume of data allows to reveal such topics only by the automated data collection methods. The automated classification is necessary as it provides an opportunity to recognize radical and extreme versions of online communities, to evaluate the range of ideological beliefs, supported by specific types of extreme right communities and promoted on online platforms.
- Extremist communities actively create and promote blogs, image boards, and web forums that share the common agenda of extreme right extremists to spread their beliefs and ideology, build a collective identity, offline and online mobilization, propaganda, and fundraising (Graham, 2013).
- The blurring of "boundaries" between extreme right movements and extremist communities, the permanent growth of new organizational hybrid forms that are not in line with the traditional schemes of the far right's formalization, but have good reasons to be classified as a motivating ideology of extreme right extremists. For example, only since 2018 the communities and individual actors promoting misogynistic ideology have begun to be classified as the extreme right ideology. This is due to the exponential growth of hate crimes and terrorist incidents in the United States, Canada and Europe committed by supporters of male supremacy (incels, MGTOW2) (Jasser et al., 2020). In addition, some researchers have noted the growth of communities that are radicalized on the platform of the extreme right, but have not yet attracted the attention of the expert community, although the incidents, committed by members of the organization known as "proud boys", have already been registered. The online communities of this organization have close ties with Alt-right, Alt-light, crypto-fascists, and misogynist communities (Kutner, 2020).
- The tactical innovation of the extreme right is that street activism has been largely replaced by Internet activism. Today's young people, who are politically active indeed, use different manipulating channels, which direct violence becomes less likely. Some scientists refer to the growing communities calling themselves Alt-light as a more intelligent movement that prefers long-term, democratic media-focused activity against forced street activism and terrorism (Ravndal, 2016).

The relevance of studying online-radicalization is increasing whereas it is neces-

sary to predict threats arising in the information field of social media under the influence of stochastic threats, differed in the nature of display, type or mechanisms of threat development. In fact, COVID-19 has created a new source of anger and cause for discontent among some part of the world's population. But the most dangerous is that this is a new trigger for future episodes of extreme right violent extremism and terrorism against targets, symbolized personal grievances projected into political discontent on racist, anti-immigration, anti-government and other grounds. Extreme right movements, in all their diverse forms, flourish on the rebound of economic crisis and harm incurred by pandemic and isolation. Having politicized pandemic, they strive to seize opportunities for rapid recruitment and mobilization of new members among anti-vaxxers, conspiracy theorists. For example, the extreme right conspiracy theorists escalated and provoked about 5G cell phone masts being used to spread the virus. That ensued the series of arson attacks on phone masts and death threats to telecom network engineers in the Netherlands and Canada (PressProgress, 2020). In the Telegram channel neo-Nazis used the doxxing technology against employees the B. Gates Foundation and WHO, having sent out their e-mail addresses and passwords in order to intimidate and provoke Internet trolling and targeted harassment with threats of physical violence offline (Kelion, 2021; Makuch, 2020). And this is only a small fraction of the "tsunami" that has fallen from the extreme right in different parts of the world, recorded in the first months of the epidemic quarantine.

Whether the technologies of promoting violent extremism, terrorism on the extreme right's ideological platform are innovatory in tactics?

Changes in the technological context hold meaning because it is the Internet as the "shadow moderator" of their simmering activity that provides the opportunity to use much of their innovation to produce bigger misdeeds to catch interest, to sow fear and terror in the masses. Consequently, it is the creation of technologies for supporting research on the mechanisms of online radicalization to solve sociological problems promptly and with big data volume becomes the primary target of researchers.

The peculiarities of the extreme right online communities and research hypothesis

In the research field the extreme right communities are more often defined as a movement or an ideological platform. But the phenomenon itself has not received a single and universal name yet. According to the generally available interpretations in the range of research materials, the common features of the extreme right communities are as follows:

− belief in the inferiority of certain and the superiority of other individuals and groups; promotion of the segregation principle: the separation of people into groups of "superior" and groups considered as "inferior" with different bases: gender, age, status, place of residence, race, etc.;

− though various extreme right communities and movements differ in many ways, they share and promote "national preferences" (hence is nationalism);

− the idea of egalitarianism: the extreme right regards social inequalities and corresponding social hierarchies as inevitable, natural, or even preferable;

− the wide landscape, we call the extreme right, relies on supremacism and nativism;

− promotion of oppressive policies, genocide, xenophobia, authoritarianism, anti-immigration and anti-integration attitudes;

− many extreme right groups believe in conspiracy theories as a serious threat to national sovereignty and/or personal freedom, as well as they keep to the conviction that their personal and/or national way of life is under the threat.

Extreme right communities choose targets as objects that they regard as enemies. They can be immigrants, minorities, political opponents or governments. Vandalism and spontaneous violence, prejudice and hatred against certain categories of people (religious, racial, gender or other motives) and the encouragement of violence are characteristic radical actions of the extreme right.

Extremist communities of the extreme right ideological platform are characterized by celebrating significant (to the community) events and persons, as well as dates associated with them.

The aim of the study is to develop the methods and automation tools to support research about online radicalization based on open data of extreme right online communities in social networks.

The hypothesis of the study is that the assessment of calendar activity of communities in the social network, if available information characterizing landmark dates for the extreme right, can be an effective tool to automate their search process and create a neural network.

Research Methodology

We conducted experimental testing of the hypothesis on the open data of the Russian social network "VKontakte" (VK). The data was extracted through the corresponding program interface of the application. The types of extracted data about online communities are name, number of subscribers, publicly available published posts for 1 calendar year.

Knowledgebase.

In order to assess the calendar activity of online communities on significant extreme right extremists' dates, an appropriate knowledge base was developed by an expert method. Table 1 provides information about the format of the content stored in the knowledge base.

We should note that it is possible to search communities of different classes with appropriate changes in the knowledge base. Filling the knowledge base with information about communities of different classes will allow to study character and force of their interrelations and mutual influence.

A calendar-correlation analysis algorithm (CCA)

To search target online communities, we designed and implemented an algorithm for calendar-correlation analysis of community activity using the content stored in a pre-formed knowledge base. The work principle of the algorithm is shown in the Fig. 1 and is as follows:

1. Inquirying the records of the analyzed community from the social network "VKontakte", using the standard method of wall.get library, for the timeframe of one calendar year.
2. Searching the records for each key date and analyzing the number of keywords occurred in the given key date. Recording the result.
3. Analyzing the community records obtained for one calendar year by the number of keywords encountered. Result is the number of each keyword occurrence in records for one calendar year, the total number of keywords encountered for one calendar year. Recording the result.
4. An expert set a threshold for the number of found records relevant to the key dates and the total number of keywords found in the community records for one calendar year.
5. Analyzing the results for exceeding the threshold.
6. Outputting the result.

Results of algorithm testing

To evaluate the efficiency of the algorithm we carried out tests.

Table 1. Knowledge base single record format

Fields name	Characteristics of the stored information
Full data	Full data Date in DD/MM/YYYY format, associated with an event significant for the ideological platform
Category	Main category (class) of the radical ideological platform, for which the date is significant
Sub-category	Additional categories of the radical ideological platform (for example: alt-right, mgotw etc.)
Keywords	Linguistic markers associated with a significant event, including named objects: personalities, places, etc.
Commentary	Expert's commentary explaining the meaning of a significant event

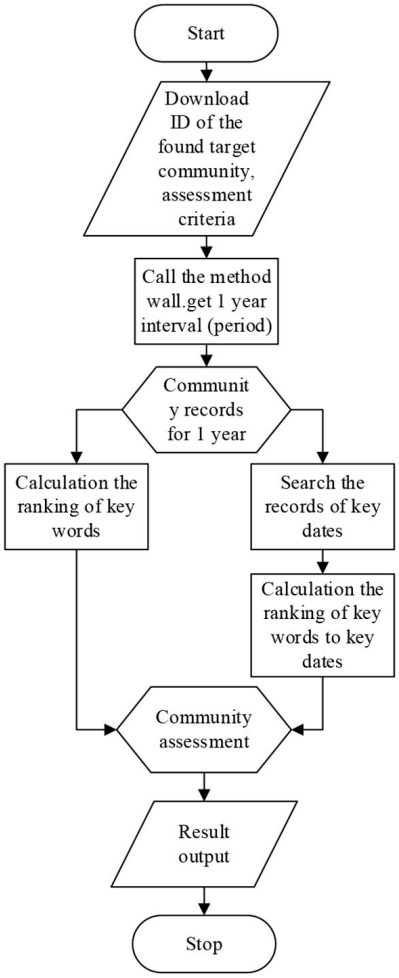

Fig. 1. Block diagram of the calendar-correlation analysis algorithm (CCA)

The first test was to search communities under prepared formalized keywords (49 words). We found 6151 communities. The communities were tested by the CCA method, which indicated only 3 communities. All of them belonged to extreme right extremist communities.

In the second testing we checked a list of 259 communities, chosen by expert method. The CCA "worked" on 49 communities from the list.

In the third testing of the algorithm, 50 popular communities were selected, which were expertly checked for the absence of the features of extreme right communities. The testing showed that the algorithm had worked only on one of these communities.

The efficiency of the algorithm can also be illustrated through the values of the first and second type errors. They can be calculated for the second and the third checks as there is no a priory information about the membership degree to the target communities from the 6151 groups found by keywords. As the null hypothesis H_0 we accept that the analyzed VK-community does not contain signs of affiliation with extreme right extremist communities. Consequently, the alternative hypothesis H_1 is that the VK-community contains signs of affiliation.

Within the second testing the hypothesis H_0 was incorrectly accepted in 210 cases, respectively the hypothesis H_1 was correctly accepted in 49 cases. Thus, the probability of the type II error is $\beta=0.81$ and the power of the criterion $(1-\beta)=0,19$.

As an additional check, type II error was estimated for each subclass of the same extreme right extremist communities. The results are shown in the Table 2.

The comparably low value of the power criterion for total communities is explained by the incomplete information provided in the knowledge base and describing the key dates and key words of the extreme right extremist communities.

In the third testing the hypothesis H_0 was correctly accepted in 49 cases, and hypothesis H_1 was incorrectly accepted in one case, i.e., the probability of the type I error is $\alpha=0,02$.

Results discussion

We interpret the relatively low accuracy of the algorithm as the result of incomplete information provided in the knowledge base. In addition, this is confirmed by the fact that for certain subclasses of the extreme right ideological platform the accuracy of the algorithm is higher. Thus, we can conclude that different classes of communities respond and honor different dates and keywords associated with them. The greater accuracy can be achieved by refining the existing knowledge base and developing rules for its addition and maintenance.

Table 2. The type II Error and power of the criterion for different classes of communities

Communities sub-class	β	(1-β)	Number of communities
Nationalists	0,375	0,625	8
Neopagans	0,91	0,09	67
Nazis	0,2	0,8	5
Alt-right	0,67	0,33	6
Manospere	0,95	0,05	19
Unidentified	0,82	0,18	154

To improve the efficiency of the algorithm through the automation of updating the information in the knowledge base, as well as to qualitatively test the hypothesis of the existence of significant community dates, we propose to use a statistical measure of the TF-IDF words significance. This will allow to test the "sensitivity" of individual subclasses of the extreme right ideological platform to dates in the knowledge base; and to identify new keywords associated with a significant event to the ideological platform.

Fig. 2 presents a sequence diagram describing the processes of assessing the "sensitivity" of the online community to a particular significant date and making changes to the knowledge base.

1. expert's request to check the "sensitivity" of a subclass of online communities to a specific date
2. request to retrieve information on a significant date
3. response to request 2
4. request to receive online community posts
5. response to request 4
6. formulating the corpus of texts for application of TF-IDF
7. processing the corpus of texts and identifying significant words, comparison of significant words with linguistic markers associated with the significant event
8. list of significant words from online community posts for the requested date

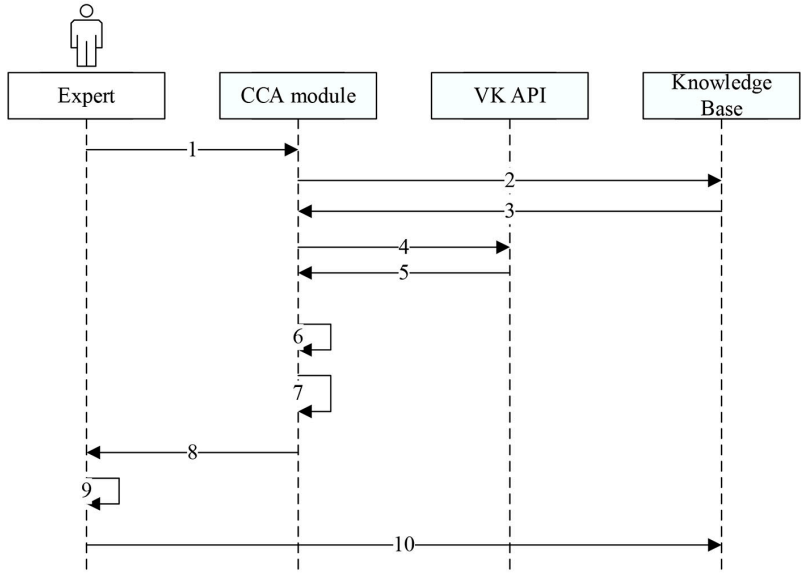

Fig. 2. Sequence diagram for assessing the «sensitivity» of the online community to a significant date

9. analysis of the result of significant words assessment

10. knowledge base update

Calculation of the significance of words for the selected date is performed by the formula:

$$weight(word, Sub) = \\ = \frac{\sum_1^n (\frac{n_{word}}{\sum_k n_k} \times log \frac{|P_{sub}|}{|\{p_i \in P_{sub} | word \in p_i\}|}}{n_{P_{sub}}}$$

n_{word} – the number of occurrences of the *word* in a post

$\sum_k n_k$ – the total number of *words* in posts

$|P_{sub}|$ – the number of posts in corpus *Sub*

Sub – the corpus of posts in extreme right online communities

$|\{p_i \in P_{sub} | word \in p_i\}|$ – the number of posts in corpus *Sub*, where *the word* occurs

Selective testing has revealed that the statistical significance of TF-IDF words is a useful tool for testing the "sensitivity" to a significant date. Table 3 demonstrates an example of testing the online communities for significant dates 07.11 (October Revolution in Russia), 07.02 (Alexander Kolchak Memorial Day) and 25.07 (Day of Solidarity with Nationalist Prisoners). The experts highlighted the words in italics as they directly related to the significant date.

Conclusion

Revealing online radicalization mechanisms is impossible in today's digital environment without reliable software, as it allows to rapidly monitor social networks. Most of the already existing algorithms in the world and Russia work on linguistic and textual analysis.

The main functions of the prototypes are based on the identification of key markers of linguistic slang of extreme right extremist communities, based on metadata (visits, publications, likes) or image properties. Such content requires that any attribute-based classifier should be linguistically formalized.

The use of modern textual analysis methods in the subject area of online radicalization research allows to match the most appropriate detection methods experimentally to the aggregated text of online communities.

Automation of the data analysis of social media involves a number of technical challenges. Firstly and more, it is necessary to single out the large volume and heterogeneity of the initial data. The task of data extraction itself is well studied in contrast to the task of finding target communities and users effectively. A potential solution could be applying the classification algorithms based on machine learning. However, their effective application is complicated by the need to generate large qualitative training and test samples of data. Depending on the applied classification algorithm, it is required samples of hundreds to thousands of communities. Otherwise, the efficiency of automatic classification can be insufficient in terms of "resources/time/quality" evaluation (Kuznetsov et al., 2021).

The development of digital technologies and their application in the Internet environment lead to large-scale, rapid changes in social sciences, in terms of new methods of collecting, processing and analyzing big data. Despite significant achievements in computational social science, we still lack technologies, methods and tools allowing to solve sociological tasks in a short time and on big data to obtain new knowledge about the mechanisms of online radicalization.

The results of the study illustrated that the data on the calendar activity of communities can be an effective method for automated

Table 3. The result of testing «sensitivity» to significant date

Date	Significant words
07.11	*revolution, freedom*, happen, *struggle,* November, president, state
07.02	*Kolchak, Pepeliaev*, matriarchy, schoolgirl, shooter, need, society
25.07	*Furgal, native of Khabarovsk,* rear, Pompeo, centrist, squadron, juror*, Khabarovsk*

assessment of affiliation with an extreme right extremist ideology if an appropriate knowledge base is available. The developed CCA algorithm can be used as an additional tool to narrow down the results received from keyword searches. CCA allows us to find the most active communities or most explicitly corresponding to the extreme right extremist ideological platform.

One of the main problems in automation of sociological research using social network data is the high labor intensity of the initial process of searching extreme right extremist communities. Adaptation of the CCA algorithm will reduce the labor intensity of the initial stage of the work and can be used much more extensively than just studying online radicalization. The results of the work can be applied, for example, as a preliminary stage for such studies as: studying and modeling the processes of information diffusion in social networks, assessing the reaction of the audience to news and events, sentiment analysis, studying the mechanisms of the social contagion phenomenon, or in studying motivational factors of political mobilization in social media.

Authors' note

All authors have agreed to the submission and the article is not currently being considered for publication by any other print or electronic journal.

References

Alperovich, V. (2020) Summary. Organizational changes on the extreme right flank: The rally activity of the extreme right. In *SOVA Center for Information and Analysis*. Available at: https://www.sova-center.ru/racism-xenophobia/publications/2020/12/d43416/

Anderson, C.W. (2012) Towards a sociology of computational and algorithmic journalism. In *New Media & Society* 15 (7): 1005–1021.

Burke, J. (2016) The Age of Selfie Jihad: How evolving media technology is changing terrorism. In *Combating Terrorism Center* 9(11). Available at: https://ctc.usma.edu/the-age-of-selfie-jihad-how-evolving-media-technology-is-changing-terrorism/

Colley, Th., Moore, M. (2020) The challenges of studying 4chan and the Alt-Right: Come on in the water's fine'. In *New Media & Society* SEP 2020. Available at: https://doi.org/10.1177/1461444820948803

C-REX (2019) Center for Research on Extremism at the University of Oslo. Available at: https://www.sv.uio.no/c-rex/english/news-and-events/news/2019/special-issue.html

Daniels, J. (2009) Cloaked websites: propaganda, cyber-racism and epistemology in the digital era. In *New Media & Society* 11(5): 659–683.

Gaudette, T., Scrivens, R., Davies, G., Frank, R. (2020) Upvoting extremism: collective identity formation and the extreme right on Reddit. In *New Media & Society* SEP 2020. Available at: https://doi.org/10.1177/1461444820958123

Global terrorism index (2019) Available at: https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2019-web.pdf

Global terrorism index (2020) Available at: https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf

Graham, M. (2013) Transnational networking on the far right: the case of Britain and Germany. In *West European Politics* 36:1:176–198.

Heide, L., Winter, Ch., Maher, Sh. (2018) The cost of crying victory: policy implications of the islamic state's territorial collapse. *ICCT.* Available at: https://icsr.info/wp-content/uploads/2019/01/ICSR-ICCT-Feature_The-Cost-of-Crying-Victory-Policy-Implications-of-the-Islamic-State%E 2 %80 %99s-Territorial-Collapse.pdf

Holt, T.J., Freilich, J.D., Steven, M., Chermak, S.M. (2020) Examining the online expression of ideology among far-right extremist forum users. In *Terrorism and Political Violence*. DOI: 10.1080/09546553.2019.1701446.

ICCT (2021) International Centre for Counter-Terrorism-The Hague. Available at: https://icct.nl/

ICSR (2020) International Centre for the Study of Radicalisation. Available at: https://icsr.info/

Jasser, G., Kelly, M., Rothermel, A.K. (2020) Male supremacism and the Hanau terrorist attack: between online misogyny and extreme right violence. *ICCT*. Available at: https://icct.nl/publication/male-supremacism-and-the-hanau-terrorist-attack-between-online-misogyny-and-far-right-violence/

Karpova, A.Y., Savelev, A.O., Vilnin, A.D., Chaykovskiy, D.V. (2019) New technologies to identify alt-right extremist communities in social media. In *Vestnik Tomskogo gosudarstvennogo universiteta-Filosofiya-Sotciologiya-Politologiya-Tomsk State University Journal of Philosophy, Sociology and Political Science* 52: 138–146 DOI: 10.17223/1998863X/52/14

Karpova, A.Y., Savelev, A.O., Vilnin, A.D., Chaykovskiy, D.V. (2020) Studying online radicalization of youth through social media (Interdisciplinary Approach). In *Monitoring of Public Opinion: Economic and Social Changes* 3:159–181 Available at: https://doi.org/10.14515/monitoring.2020.3.1585

Kelion, L. (2021) Coronavirus: 20 suspected phone mast attacks over Easter. *BBC News*. Available at: https://www.bbc.com/news/technology-52281315

Kemp, S. (2020) Digital 2020: 3.8 Billion people use social media. In *We are social*. Special reports. Available at: https://wearesocial.com/blog/2020/01/digital-2020–3–8-billion-people-use-social-media

Kutner, S. (2020) Swiping Right: The allure of hyper masculinity and cryptofascism for men who join the proud boys. *ICCT* Research Paper. Available at: https://icct.nl/app/uploads/2020/05/Swiping-Right-The-Allure-of-Hyper-Masculinity-and-Cryptofascism-for-Men-Who-Join-the-Proud-Boys.pdf

Kuznetsov, S.A., Karpova, A.Y., Savelev, A.O. (2021) Automated detection of ultra-right communities' cross-links in a social network. In *Vestnik Tomskogo gosudarstvennogo universiteta-Filosofiya-Sotciologiya-Politologiya-Tomsk State University Journal of Philosophy, Sociology and Political Science* 59: 156–166 DOI: 10.17223/1998863X/59/15

Levada Center (2019) Monitoring xenophobic attitudes. Available at: https://www.levada.ru/2019/09/18/monitoring-ksenofobskih-nastroenij-2/

Lewis, R. (2018) Alternative influence: broadcasting the reactionary right on YouTube. *Data & Society.* Available at: https://datasociety.net/wp-content/uploads/2018/09/DS_Alternative_Influence.pdf

Makuch, B. (2020) Neo-nazis are spreading a list of emails and passwords for gates foundation and WHO employees. In *VICE Media Group*. Available at: https://www.vice.com/en_us/article/akwxzp/neo-nazis-are-spreading-a-list-of-emails-and-passwords-for-gates-foundation-and-who-employees

Munich Security Report (2020) The Munich Security Conference 2020, 14–16 February. Available at: https://securityconference.org/assets/user_upload/MunichSecurityReport2020.pdf

Poole, E., Giraud, E.H., Quincey, E. (2021) Tactical interventions in online hate speech: The case of #stopIslam. In *New media and Society* 23(6): 1415–1442.

PressProgress (2020) Canada's Anti-Lockdown Protests are a Ragtag Coalition of Anti-Vaccine Activists, Conspiracy Theorists and the Extreme right. Available at: https://pressprogress.ca/canadas-anti-lockdown-protests-are-a-ragtag-coalition-of-anti-vaccine-activists-conspiracy-theorists-and-the-far-right/

Ravndal, J.A. (2016). Right-wing terrorism and violence in Western Europe: Introducing the RTV dataset In *Perspectives on Terrorism* 10.

Siebe, T.M. (2019) *Digital transformation: survive and thrive in an era of mass extinction*. New York: RosettaBooks.

START (2020) National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland. Available at: https://www.start.umd.edu/

Tang, L., Liu, H. (2010) Community Detection and Mining in Social Media. In *Synthesis Lectures on Data Mining and Knowledge Discovery* 2(1): 1–137.

Wahlström, M., Törnberg, A., Ekbrand, H. (2020) Dynamics of violent and dehumanizing rhetoric in extreme right social media. In *New media and Society* August 2020 Available at: https://doi.org/10.1177/1461444820952795

Yudina, N. (2020) Summary. Criminal activity of the extreme right. Hate crimes and countering them in Russia in 2019. In *SOVA Center for Information and Analysis*. Available at: https://www.sova-center.ru/racism-xenophobia/publications/2020/02/d42015/