social sciences

MDPI

Article

Method for Detecting Far-Right Extremist Communities on Social Media

Anna Karpova [1,*], Aleksei Savelev [2], Alexander Vilnin [2] and Sergey Kuznetsov [2]

[1] Division for Social Sciences and Humanities, School of Core Engineering Education, National Research Tomsk Polytechnic University, 634050 Tomsk, Russia
[2] Division for Information Technology, School of Computer Science & Robotics, National Research Tomsk Polytechnic University, 634050 Tomsk, Russia; sava@tpu.ru (A.S.); vilninad@tpu.ru (A.V.); ksa11@tpu.ru (S.K.)
* Correspondence: belts@tpu.ru

Abstract: Far-right extremist communities actively promote their ideological preferences on social media. This provides researchers with opportunities to study these communities online. However, to explore these opportunities one requires a way to identify the far-right extremists' communities in an automated way. Having analyzed the subject area of far-right extremist communities, we identified three groups of factors that influence the effectiveness of the research work. These are a group of theoretical, methodological, and instrumental factors. We developed and implemented a unique algorithm of calendar-correlation analysis (CCA) to search for specific online communities. We based CCA on a hybrid calendar correlation approach identifying potential far-right communities by characteristic changes in group activity around key dates of events that are historically crucial to those communities. The developed software module includes several functions designed to automatically search, process, and analyze social media data. In the current paper we present a process diagram showing CCA's mechanism of operation and its relationship to elements of automated search software. Furthermore, we outline the limiting factors of the developed algorithm. The algorithm was tested on data from the Russian social network VKontakte. Two experimental data sets were formed: 259 far-right communities and the 49 most popular (not far-right) communities. In both cases, we calculated the type II error for two mutually exclusive hypotheses—far-right affiliation and no affiliation. Accordingly, for the first sample, $\beta = 0.81$. For the second sample, $\beta = 0.02$. The presented CCA algorithm was more effective at identifying far-right communities belonging to the alt-right and Nazi ideologies compared to the neo-pagan or manosphere communities. We expect that the CCA algorithm can be effectively used to identify other movements within far-right extremist communities when an appropriate foundation of expert knowledge is provided to the algorithm.

Keywords: online radicalization; far-right; extremism; terrorism; social media analytics; big data; web mining

Citation: Karpova, Anna, Aleksei Savelev, Alexander Vilnin, and Sergey Kuznetsov. 2022. Method for Detecting Far-Right Extremist Communities on Social Media. *Social Sciences* 11: 200. https://doi.org/10.3390/socsci11050200

Academic Editors: Matthew Valasik and Shannon E. Reid

Received: 15 March 2022
Accepted: 28 April 2022
Published: 2 May 2022

1. Introduction

Researchers' interest in the intellectual analysis of destructive social media content, including collecting, processing, and interpreting web content to predict youth radicalization and prevent extremist- and terrorist-oriented incidents, has shown steady growth in the last decade. Young people are in the risk group and are the most vulnerable population category to the destructive information and psychological influence of radical communities. Extremist and terrorist groups effectively use artificially manipulated tools to

engage youth through social networks and video sharing sites. Social networks' widespread availability and popularity allow ultra-radical communities to use networks to plan and mobilize users to commit unlawful acts.

A predictor of violent incidents of an extremist, terrorist nature is radicalization (LaFree 2013). Although radicalization has become a frequently used concept in studies of terrorism and violent extremism over the past two decades, the idea is not uniformly interpreted and does not even fit within any academic discipline (Borum 2011). A fundamental marker for conceptualization is the understanding of radicalization as a transition process from non-radical to radical forms. According to researchers, there is no single pathway to radicalization, nor is there a single profile of person who accepts the idea that a violent way of achieving a goal is the only possible (and justified) way to solve a problem (Hofmann 2018).

In general terms, radicalization is understood as a gradual step-by-step process of escalation from nonviolent forms of expression to more violent forms of behavior and willingness to take violent action (Borum 2004; McCauley and Moskalenko 2008; Garcet 2021). Radicalization is a complex set of causal factors and processes in which several factors work together to produce extremist and terrorist incidents. The criterion for ultra-radical actors and the legal assessment of community actions is to assess the level of their methods' risk to both society and the state and whether these actions fall under the legislation of different countries. They justify and promote this line, express their willingness to switch to violent acts, and assume a moral obligation to protect those groups that promote this idea.

The Internet brings new opportunities to ultra-right communities for promoting their ideology in a multitude of ways. It is a crucial technological innovation that allows the achievement of ideological, political, economic, and other goals. The improvements in communication channels and the spread of social services enable unprecedented speed and density of communication. In January 2022, there were around 4.66 billion Internet users worldwide (60.1% of the world's population) (Johnson 2021).

Radicalization is now taking on a massive, viral, scalable effect due to new communication technologies via social media (Hall et al. 2019; Borum 2011; McCauley and Moskalenko 2008, 2017; Michael A. Jensen et al. 2018). Furthermore, the number of active social media users has reached 4.1 billion (53.5% of the world's population) (Statista Research Department 2022). However, the Internet itself is not the cause of radicalization but a contributing factor to a person's drive to commit violent acts. In this regard, a diagnostic tool such as "social media analytics", an interdisciplinary research area that aims to combine, extend, and adapt social media analysis methods, is of great importance (Sureka and Agarwal 2014; Xie et al. 2016; Conway 2017; Gilani et al. 2017; Stieglitz et al. 2018; Savelev et al. 2021; Karpova et al. 2020).

Adapting modern information technology for subject matter purposes provides digital transformations to solve sociological problems more quickly and with larger amounts of data (Anderson 2012; Weiler et al. 2016; Barhamgi et al. 2018; Wendelberg 2021). The effectiveness of the digital transformation depends directly on organized collaboration between data scientists, subject matter experts, and professional service providers who supply cloud storage, digital platforms, and software development (Siebel 2019). For the purpose of the current work we define online radicalization as a social and psychological transformation process in which an individual adopts an extremist belief system that prepares the ground for offline violence. The quintessential process is the destructive information and psychological influence (DIPI) on social media users in the online environment through the use of information and communication technologies to achieve ideological, political, economic, and other goals (Karpova et al. 2019, 2020; Kuznetsov et al. 2021).

The goal of this work is to present a new method of calendar-correlation analysis (CCA) for identifying far-right communities on social media. This method allows the automation of the search process for the study of online radicalization. To achieve our goal, we began by reviewing the state of current research to identify key opportunities and

limitations in creating automated tools. The second part of the paper describes the design process and software implementation of parametrized social media–content retrieval and the methodology for creating a "knowledge base" for the prototype. The third part of the paper focuses on our research design and describes the CCA algorithm. Our method combines the speed of computer data analysis, a mathematical model for identifying a target group by a characteristic change in a social media community activity around critical events, and a knowledge base. In the fourth part of the paper, we outline research strategies to test our methodology. Finally, we outline the potential applications of the CCA and the prospects for future work on prototyping a system to automate research on online radicalization studies.

2. State-of-the-Art

In 2018, the International Centre for the Study of Radicalisation (ICSR) highlighted in its report that "in recent years, IS-inspired terrorism has absorbed the lion's share of law enforcement and intelligence resources-and rightly so, given the extent of the group's menace. However, this has come at the cost of investing those resources elsewhere. Meantime, far-right extremist groups have been developing and mobilizing across Europe" (Heide et al. 2018). Researchers at the International Center for Counter-Terrorism (ICCT), the National Consortium for the Study of Terrorism and Responses to Terrorism (START), and the Center for Research on Extremism (C-REX) supported this view. In its 2020 report (PST 2020), the Norwegian Security Service noted the threat of right-wing extremism. The Dutch Foreign Intelligence Service also pointed to the growing threat of right-wing extremism in its 2019 annual report (AIVD 2019).

The 2020 annual report of the world's most significant Munich International Security Conference experts stated that right-wing extremism is a crucial question on the agenda along with space security, climate security, and the technological race (MSC 2020). According to the Institute for Economics and Peace: (1) over the last 8 years, people, motivated by radical right-wing ideology have committed almost three times more terrorist attacks than Islamists (GTI 2020); (2) the number of cases of far-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 (GTI 2020); (3) the three most significant politically motivated terrorist incidents in the West for the last 50 years were perpetrated by the far-right (GTI 2019); (4) the increasingly decentralized nature of both the global Islamist and far-right movements is mainly due to the growth of the online extremist ecosystem (GTI 2019; Gaudette et al. 2020); and (5) extremist groups flourish in crisis narratives, but digital analysis demonstrates how the ways of using the pandemic for extremist purposes are changing and growing (GTI 2020). Thus, this indicates a growing trend of vulnerable young people involved in extremist and terrorist far-right communities.

2.1. The Peculiarities of Far-Right Extremist Communities

Researchers often define far-right communities in the research field as movements or ideological platforms. However, the phenomenon itself has not received a single, universal name yet. According to the generally available interpretations in the range of research materials, the standard features of the far-right communities are as follows:

- belief in the specific inferiority and the superiority of other individuals and groups; promotion of the segregation principle: the separation of people into groups considered "superior" and groups considered "inferior", with different bases: gender, age, status, place of residence, race, and others;
- though various far-right communities and movements differ in many ways, they share and promote "national preferences" (hence, nationalism);
- the idea of egalitarianism: the far-right regards social inequalities and corresponding social hierarchies as inevitable, natural, or even preferable;
- the broad landscape we call the far-right relies on supremacism and nativism;

- promotion of oppressive policies, genocide, xenophobia, authoritarianism, anti-immigration and anti-integration attitudes;
- many far-right groups believe in conspiracy theories as a severe threat to national sovereignty and (or) personal freedom, and they also maintain the conviction that their personal and (or) national way of life is under threat.

Vandalism and spontaneous violence, prejudice and hatred against specific categories of people (religious, racial, gender, or other categories) and the encouragement of violence are characteristic radical actions of the far-right. Far-right communities target those they regard as enemies. They can be immigrants, minorities, political opponents, or governments.

2.2. Far-Right Online Radicalization: Specifics of the Study

One can apply radicalization's theoretical concepts and empirical evidence (both for individuals and for groups) from worldwide studies specifically to Russian social networks only with significant adaptation. The international research field has accumulated experience in this area, developed the concept and models of radicalization (McCauley and Moskalenko 2008, 2017; Neumann 2009; Braniff 2017; Hamm and Spaaij 2015), and created databases of radicals and services (PIRUS, BAAD, IVEO, TEVUS, GTD). However, application programming interfaces (APIs) and the rules for their use for data collection from social networks differ significantly (for example, comparing VKontakte and Facebook). Therefore, for research on popular social networks in Russia, the available foreign software analogs should be adapted to the API capabilities and specific research tasks.

The next challenge is to explore how new technologies are used for promoting far-right ideological platforms, the complexity of which is related to two groups of factors: (1) theoretical and methodological, and (2) instrumental. These two groups are related to the possibilities and limitations of intelligent analysis of social network data as a tool for automating research in the subject area of study.

In the first group of factors, theoretical justification is of crucial importance. The concept of radicalization is still under formation and has complex theoretical explanations. Radicalization has a complex set of causal relationships and does not lend itself to universal formalization. A narrowly defined subject spectrum (e.g., only religious radicalization or limitations in variables, i.e., studying only those who have committed incidents and excluding the near-radical environment which formed their violent beliefs) creates research gaps where data are scarce or non-existent, and rigorous methods are lacking. In such cases, researchers do not link results to theoretical frameworks. C-REX researchers emphasize that the research field remains rather diverse, unorganized, and fragmented. Each country uses different definitions, different recording methods, and different criteria. Methods and criteria change from time to time, making time-series analysis difficult.

Statistics are of limited value because they are ultimately incomparable (Ravndal and Bjørgo 2018). The problem of classifying the different forms of ideological organization of far-right communities and the new hybrid forms of growth is also significant. There is a blurring of the "boundaries" between radical movements and communities, with the permanent growth of new organizational hybrid forms that do not fit into the usual schemes of formalization—belonging to a specific ideology (leading to the intertwining of ideologies). For example, since 2018, communities and individual actors promoting misogynistic ideologies have begun to be classified as far-right ideologies. The reason is the exponential growth of hate crimes and terrorist incidents in the United States, Canada, and Europe committed by supporters of male supremacy—incels and MGTOW (Jasser et al. 2020). In addition, some researchers have noted the growth of radicalized communities on the far-right platform that have not yet attracted the attention of the expert community. However, the incidents committed by members of the organization known as "the Proud Boys" have already been registered by researchers. The online communities of this organization have close ties with alt-right, alt-light, crypto-fascists, and misogynist communities (Kutner

2020). The C-REX classification noted the broadest range of ideological beliefs espoused by the far-right. They justify the division into radical and extreme versions of far-right movements and define three types: cultural, ethnic, and racial nationalism. Radical movements aim for change within a democracy; extreme movements reject democracy and promote violence or other illegal or undemocratic means as legitimate (Bjørgo and Ravndal 2019).

Nevertheless, despite the theoretically sound classification, the authors emphasize that these categories are instead "ideal types" and that the distinctions may be less clear-cut for specific groups. Furthermore, the authors point out that there is cooperation between groups from different ideological camps, and the differences serve as a starting point for understanding the far-right in order to assess the different goals and potential threats they pose (Ravndal and Bjørgo 2018; Bjørgo and Ravndal 2019). An automated classification tool is needed to recognize and assess the range of ideological beliefs that specific types of far-right communities espouse and promote on online platforms. Furthermore, here the theoretical- and methodological- level factors are intertwined with the instrumental factors, where the goal is automating data analysis tasks to reduce the need for an expert without compromising the quality of the analysis results. In all data mining tasks, including data transformation, feature reduction, algorithm selection, post-processing, and data interpretation, subject matter knowledge is a pressing need (Wadhwa and Bhatia 2013). An expert must assemble subject matter knowledge represented in ontological models that machines can process and formalize for these purposes. Examples of creating ontologies in the subject area of terrorism studies already exist, such as the low-level ontology "Terrorist-Personality" (Turner 2011). Meaningful work is emerging in radicalization studies that use a subject–domain ontology to perform intelligent analysis of social network data. For example, OFEDR, an ontological framework for facilitating the early detection of radicalization, is based on applying a semantic approach to finding indicators of radicalization in social networks (Wendelberg 2021).

One of the most well-known aspects of social media is adapting the content appearing in users' channels, addressing their specific values and interests, and inserting it into their like-minded networks. This feature makes it a key asset for extremist and terrorist groups. In the physical and virtual worlds, such groups notedly rely on the isolation of potential recruits from views and opinions that diverge from their prevailing beliefs. Far-right communities strive for including people in "echo chambers" that strengthen their messages and reject any opposing opinions. Thus, online communities, by their nature, create an environment that promotes radicalization for their users. Far-right communities rapidly developed the use of social media 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 and, in fact, provide a cyber transition between traditional moderate discourse and the radical rhetoric of "hate speech" (Holt et al. 2020). For example, the creators of AIN (YouTube's alternative influence network) strive to provide an alternative source of information to young disappointed media consumers, give a sense of countercultural rebellion, express distrust of "leading" news media, and frame the content as carefree, interesting, rebellious, and fun. Instead of selling a product or service, they sell political ideology by applying marketing techniques. Such sites radicalize the audience by transmitting mainstream to extremist content via guest statements and crosslinks. Online discussion presenters themselves (academics, media experts, and Internet celebrities) often move to more radical positions and subsequent interactions with other influential individuals in far-right communities, promoting and advertising radical ideological beliefs. In general, AIN disseminates far-right content, using influence to purposefully create a common countercultural identity (Lewis 2018).

In recent years, far-right communities on the Internet have co-opted the use of memes (which synthesize pop culture, ideological and political beliefs, and irony into one image)

to create engaging viral content. Far-right extremist memes spread on Gab or 8chan (considered far-right platforms) and on Instagram, Reddit, YouTube, and FacebookLive. Of particular note is the tactical innovation of the far-right known as doxxing, i.e., publishing personal information on the Internet. One of the most vivid examples was the doxxing attack on American journalist Luke O'Brien, who published an article revealing the identity of the author of a far-right American account that was highly influential and known for making Islamophobic and migrantophobic statements. O'Brien was doxxed and trolled by the far-right and Islamophobes. Among the posts against him were threats of murder as well as physical, professional, or financial harm. The attacks targeted O'Brien and his colleagues, family members, and several other unrelated individuals named Luke O'Brien. The victim's posted data is then spread by users to many other platforms. This case demonstrates two trends: the cross-platform coordination of online trolling as targeted harassment, both online and in real life, with threats of physical violence, and the aggressive, coordinated actions of the extreme right and its supporters. Changes in the technological context hold meaning because the Internet is the "shadow moderator" of their simmering activity, which allows them to use much of their innovation to produce more significant misdeeds to generate interest and sow fear and terror in the masses. Studying how to promote such content is a separate task, both in selecting and improving the methodology and solving the instrumental problem (Hashemi and Hall 2019).

Several methodological factors entailing problems of far-right online radicalization forecasting are related to the problem of ground truth. Researchers usually cannot verify sociodemographic parameters and geolocation data with high accuracy. Static data specified in the user profile often cannot be verified. It is necessary to consider and understand which data we can trust for the design of research. Another problem is the verification of connections between communities based only on subscribers. This is a crowd-sourced statistic. Researchers can not accurately measure how many accounts represent real users (many accounts have restricted access), for what reason the user subscribed to the community (perhaps he follows his ideological opponents), how much real attention the user pays to the content, etc. We should not forget about subscriber accounts for scamming (software bots). The very task of identifying and filtering software bots is already nontrivial. Today, researchers are exploring ways to assess the impact of software bots (Forelle et al. 2015; Varol et al. 2017; Stella et al. 2018; Rahwana et al. 2020; Whiting et al. 2021). Software bots have varying levels of sophistication. Efficient bots exhibit activity that humans cannot distinguish. Bots are "getting smarter." We need to understand how they affect research results. For example, what is the content focus if a bot participates in comments? Who is promoting the topic and for what purpose? It is not enough to filter them out. We still need to understand the nature of the bot. Even if one uses the available bot-filtering tools (Botometer 2021), researchers have to understand that services do not disclose the mechanics of their work, so it is challenging to assess the effectiveness of their work because researchers need to perform reverse engineering.

Bots themselves require the close attention of both subject matter experts and data scientists. A prerequisite is the selection, adaptation, and improvement of software bot classification methods based on the application of mixed methodologies combining expert human knowledge with ML (machine learning), DL (deep learning), NLP (natural language processing), and A.I. (artificial intelligence) systems. Moreover, we again encounter instrumental factors in this context—creating tools to identify and filter software bots and theoretical and methodological ones.

2.3. Key Opportunities and Limitations in the Creation of Automated Online Radicalization Research Tools

Today, it is impossible to study the radicalization process to the full extent by excluding the data that is publicly available on social networks. At the same time, some factors significantly influence the efficiency of the automation of online radicalization research.

We have conventionally classified them into three primary levels, reflecting the sequence of data analysis:

1. Data extraction–level limitations. The primary 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, and others. Using several social media as primary data sources entails multi-agent acquisition subsystem development. Apart from being technically challenging, especially for small research teams, it also means that we depend entirely on social media owners;
2. Data processing–level limitations. Despite the extraordinary amount of publicly available data on social media, the amount is still insufficient. There is no explicit information about the nature of the connections between users and communities. There is no possibility of verifying 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 a situation where we cannot ignore the available online information as it can potentially improve the accuracy of the scientific worldview, but we also cannot base decisions solely on online data;
3. Data interpretation–level limitations. The development of artificial intelligence methods and their accompanying use increases the qualification requirements for researchers. Additional competence in development programs and new educational trajectories are necessary in this case, but a qualitative formalization of accumulated experience and knowledge allows the transit to algorithm development.

2.4. Far-Right Extremist Communities in Russia

In Russia, systematic monitoring studies of far-right extremist communities are not conducted. We gather information about these communities' dynamics, evolution, or stagnation from scattered social media sources. There are no open official statistics publications with in-depth analyses of incidents. Many incidents often do not fall into the headlines, or journalists rely on poor (unverified) sources in their reporting. The circumstances of the incidents remain largely vague.

The experts from the Centre for Information and Analysis on Nationalism and Xenophobia note in their report that (Yudina 2020), according to official data, the number of hate crimes, i.e., those criminal offenses committed for ethnic, religious, or similar reasons or bias, has decreased in Russia for the last 10 years. It is not easy to estimate the true extent of the situation. Since the media often suppresses such incidents, information is fragmented, and crimes are covered such that it is impossible to understand whether hate-based motives or other reasons cause them. Hate-motivated incidents were recorded in 18 regions of the Russian Federation in 2019 and 12 regions in 2018. Attacks on "ethnic outsiders" remain the dominant category, with the second group being crimes against political and ideological opponents. During 2019, there was an increase in the number of attacks on members of LGBT communities. (Yudina 2020). According to the 2019 report by public opinion research experts (Pipiya 2019), considerable mass unrest with ethnic overtones increases xenophobia. The expert noted incidents against such ethnic communities as the Roma (Pipiya 2019). Furthermore, a few more critical markers with which experts characterized far-right activism in Russia in 2019–2020 are as follows:

- There was a decline in criminal activity but a growing share of more dangerous violence;
- Hate crimes have become even more concealed;
- At least 45 people suffered from racist and other ideologically motivated violence;
- The number of right-wing attacks on political, ideological, or "stylistic" opponents was significantly lower than the year before;
- The number of attacks on ideological sites decreased;

- The proportion of dangerous acts—explosions and arson—increased during the year;
- The theme of the threats from the far-right remained topical; photos, personal data of anti-fascists, left-wing activists, independent journalists, and law enforcement officers, and threats against them appeared on the social media pages of these organizations and groups.

In 2020, there was a surge of street activity in rallies and protests, and a continued decline in the number of Russian march participants that began 2014. At the same time, experts note that the share of activity in election campaigns has remained consistently high in recent years as it does not require significant resources and, compared to rally activity, most importantly, it does not require interaction with the authorities (Yudina 2020).

2.5. Specific Markers for the Promotion of Far-Right Extremist Ideology in the Online Environment

Before describing specific markers, let us briefly outline the characteristics and reasons why we chose the social network VKontakte for the study. Most of the results published in scientific periodicals related to the study of the promotion of far-right extremist ideology in the online environment, as well as the very creation of tools for their study, are aimed at popular social networks, messengers, video hostings, and image boards such as Facebook, Telegram, Twitter, YouTube, Gab, 8chan, and others. Nevertheless, the social network Vkontakte is the most in-demand platform for youth interaction in the Russian social media field. As of October 2021, the total number of authors (users who publish at least one public message per month) in the Russian segment of social networks reached 66.4 million. The total number of published messages is 1.1 billion. Of these, VKontakte accounts for 23.8 million authors and 408.8 million messages. Age is indicated by 45.25% of the authors, with the largest segment being from 25 to 34 years old (29% of the authors who indicated age), with the second largest being 18 to 24 years old (19.2%), and the third being from 35 to 44 years old (21.8%). At the same time, 54.9% of the authors indicated their gender as female and 45.1% as male. The activity rate of the authors is 17.2 publications per year (Cherniy 2021). VKontakte is a social network without pre-moderation of the content posted by users. At the same time, there is an automated search for content, the distribution of which in the territory of the Russian Federation is prohibited by a court decision. There is also a mechanism for users to file complaints about the content posted (e.g., offensive content). In some cases, filing a complaint may lead to the subsequent blocking of content. We chose Vkontakte for the study for several reasons. First, it is the platform with the most significant number of users in Russia. Second, as has been noted by several researchers (Reuter and Szakonyi 2015; Sanovich et al. 2018; Urman 2019; Kozitsin et al. 2020; Golikov 2021; Poupin 2021), this platform is a virtual channel for mass distribution of destructive and illegal information, a platform for protest mobilization, and a resource for promoting far-right extremist ideology. Third, the VKontakte API has significantly fewer limitations than Facebook, Telegram, and Twitter APIs. These reasons allow us to collect data for a representative sample for a significant number of criteria. Fourth, as a Russian research group, we are interested in making sense of the problem of far-right online radicalization in the context of our reality.

To study the specific markers of the promotion of far-right extremist ideology in the online environment, we relied on studies published in scientific periodicals over the past 10 years. One identifies the following markers as the analysis result:

- The construction of a collective identity to maintain group cohesion and attract new members;
- Extrapolation of radical prejudices (e.g., racism) into "rational" claims focused on ethnic, national, linguistic, and religious minorities;
- Funding of individual values and motives that can stimulate active involvement in far-right communities;

- Seeking significance and status;
- Networking with like-minded individuals for offline and online mobilization and recruiting new members;
- The crucial role of ideology in justifying violent action;
- Charismatic leadership as a stimulus to increase organizational strength;
- Background conditions—social, political, economic, and others.

The specific marker identified by subject matter experts during the initial search study of far-right extremist communities in the VKontakte social network is "staples" in the form of dates, events, personalities, and heroic figures through which activists awake discussions, activate, and attract new community members (Karpova et al. 2019; Kuznetsov et al. 2021). In the process of discussing such "scrapes", participants are heated up by provocative and aggressive statements, inciting hatred, and using "hate speech". In fact, such "staples" allow community members to distinguish participants along the lines of a "friend-or-foe" demarcation, which allows community moderators to eliminate "outsiders" and involve "insiders", thereby building up resources.

3. The Architecture of the VKontakte Social Network Analysis System

We designed and implemented software to automate the detection of far-right communities in the VKontakte social network. Figure 1 represents the high-level architecture of the software. According to the user agreement, we extracted raw data using *VKontakte API* (VK API) methods—the only possible way to work with social network data. Access rights to user and community accounts were defined using access *tokens* provided by the social network. Access to "private" profiles is only possible if the researcher's account token has the appropriate permissions. In practice, this means that the profile administrator must approve the account (add it to the subscriber list). Part of the extracted raw data is stored in an appropriate data repository to speed up processing. Personal data is not collected and processed following Russian law. Thus, raw data for processing is combined into a data mart from the data storage and extracted directly through VKontakte. Three logical blocks represent the data processing functions. The *Search Engine* provides the functionality of a parameterized data search in the social network. It is possible to search by keywords and additional filters, such as the date of the last activity within a profile, the number of subscribers, and others. The *Stats Engine* provides the ability to process quantitative data. The *Content Mining Engine* includes several methods to process published content. On the one hand, the knowledge base contains descriptive information about different types of far-right ideological platforms. On the other hand, it stores several tagged data sets, including information on significant named entities, platform-specific terminology, personalities, important events, and dates.

The primary filling of the knowledge base was performed in three main stages. The first stage was the formation of linguistic marker (keywords) dictionaries. The dictionaries included specialized words and phrases that far-right extremist communities use for communication, propaganda, promotion, abbreviations, numerical symbols, slogans, and calls for violent action, i.e., all the semantic units identified as manifestations of hate speech. The data sources were: The Ministry of Justice of the Russian Federation Federal List of Extremist Materials (Minjust 2021); the List of Public and Religious Associations and other non-profit organizations (NAC 2021) against which there is an enforcement decision to liquidate or prohibit their activities on grounds provided by the federal law "On Counteraction to Extremist Activity"; and the dictionary of extremist slogans, developed by the experts of the Laboratory of Expert Research and Situation Analysis, Moscow, Russian Federation. The second stage was the search for related communities (satellites). In order to identify the relationship between far-right extremist communities and other communities, one implements a procedure to search for satellite communities, the feature of which is the simultaneous membership of their members in both communities. The basis of the

method is the use of the list of already identified far-right extremist communities and corresponding VKontakte API functions. An expert performs the extraction of new, previously unknown linguistic markers to populate the knowledge base.

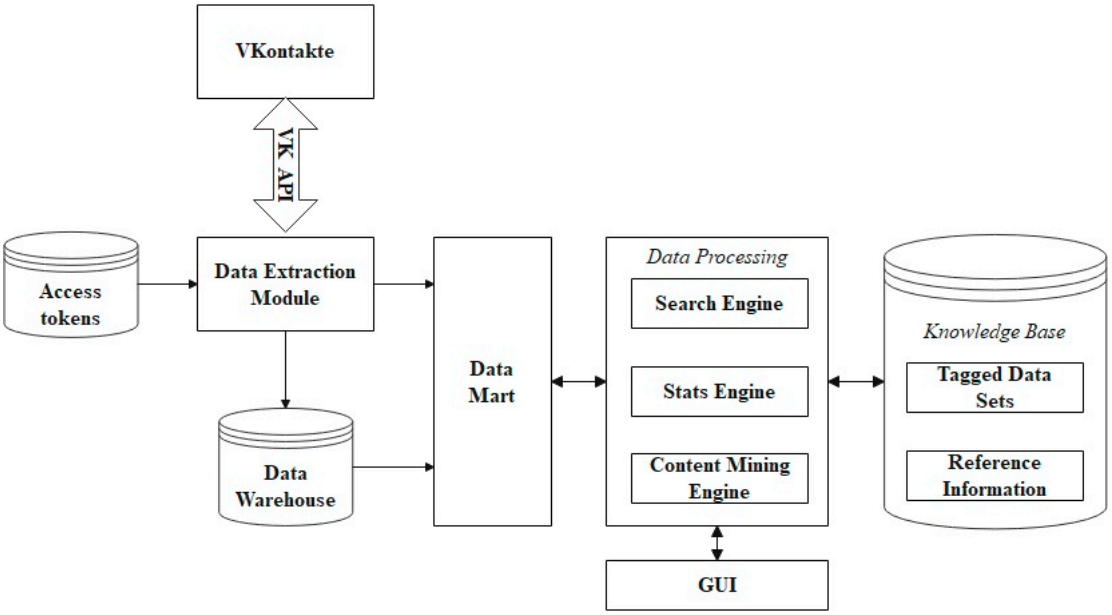

Figure 1. Software architecture for automated detection of far-right communities in the social network VKontakte.

4. The Calendar-Correlation Analysis (CCA) Algorithm of Social Network Community Activity

As a tool for the automated search of far-right online communities in the social network VKontakte, we proposed assessing calendar activity around important dates for the relevant ideological platforms (calendar-correlation analysis). The software method was based on the implementation of the following factors:

(a) It is not possible to extract retrospective data on community activity, and it is only possible to estimate the total number of views, likes, reposts, and comments since the publication date of the post;
(b) The community may show abnormal activity compared to regular activity before a significant date and after;
(c) Community activity on significant dates can be random or standard, and this is the case not only for radical communities.

We calculated the relative activity of target communities in the VKontakte social network as follows:

$$A_{rel}(d) = \frac{(2K+1)A_{abs}(d)}{\sum_{i=d-k}^{d+k} A_{abs}(i)}$$

where:

A_{abs}—absolute community activity, which is a superposition of views, likes, comments, and reposts;
d—an important date for the far-right ideological platforms;
k—a variable to denote the boundaries of the time interval in question.

Figures 2 and 3 represent the examples of absolute and relative activity graphics of the far-right online community. The developed CCA algorithm makes it possible not only to extract absolute values of community activity but also to normalize them and further refine the nature of the activity (each important date corresponds to a set of keywords and

expressions associated with it). This technique ensures better accuracy in identifying far-right extremist communities.

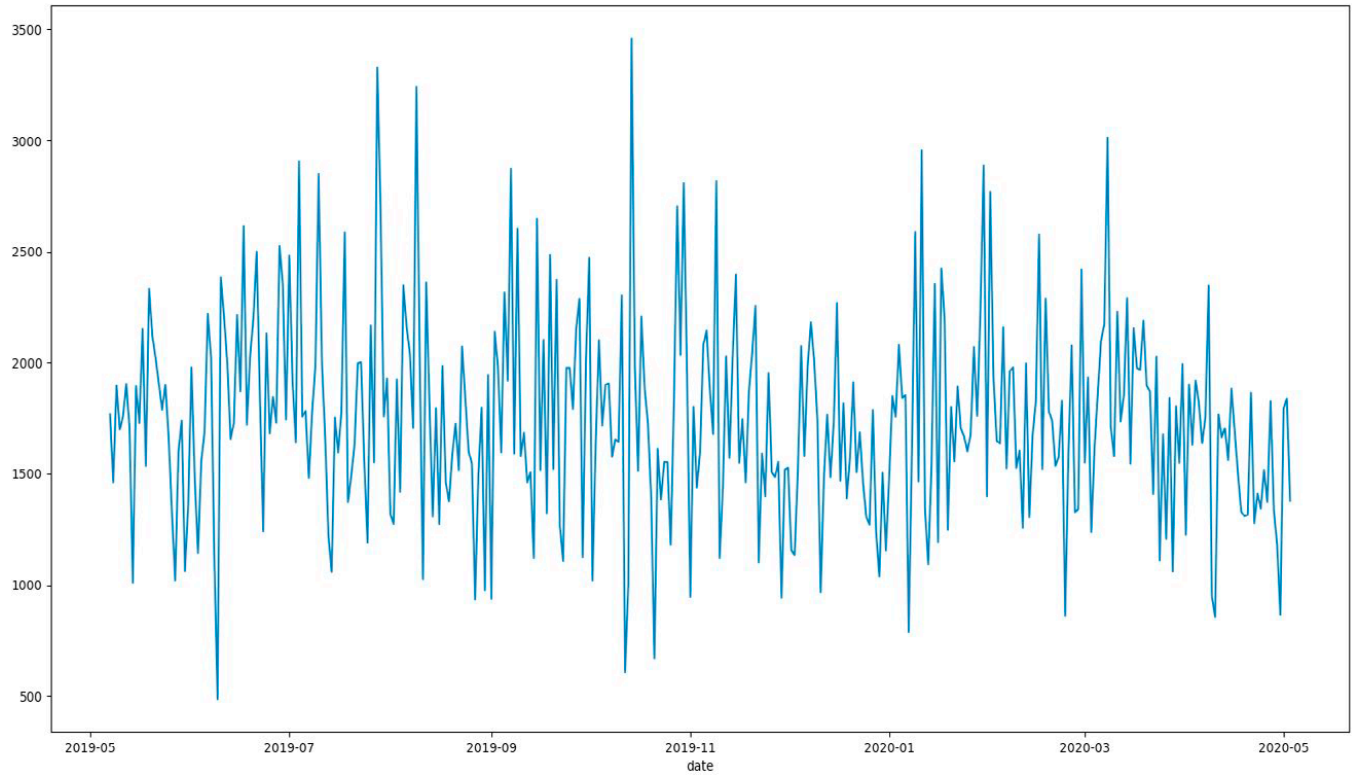

Figure 2. An absolute activity graph example of the far-right VKontakte community.

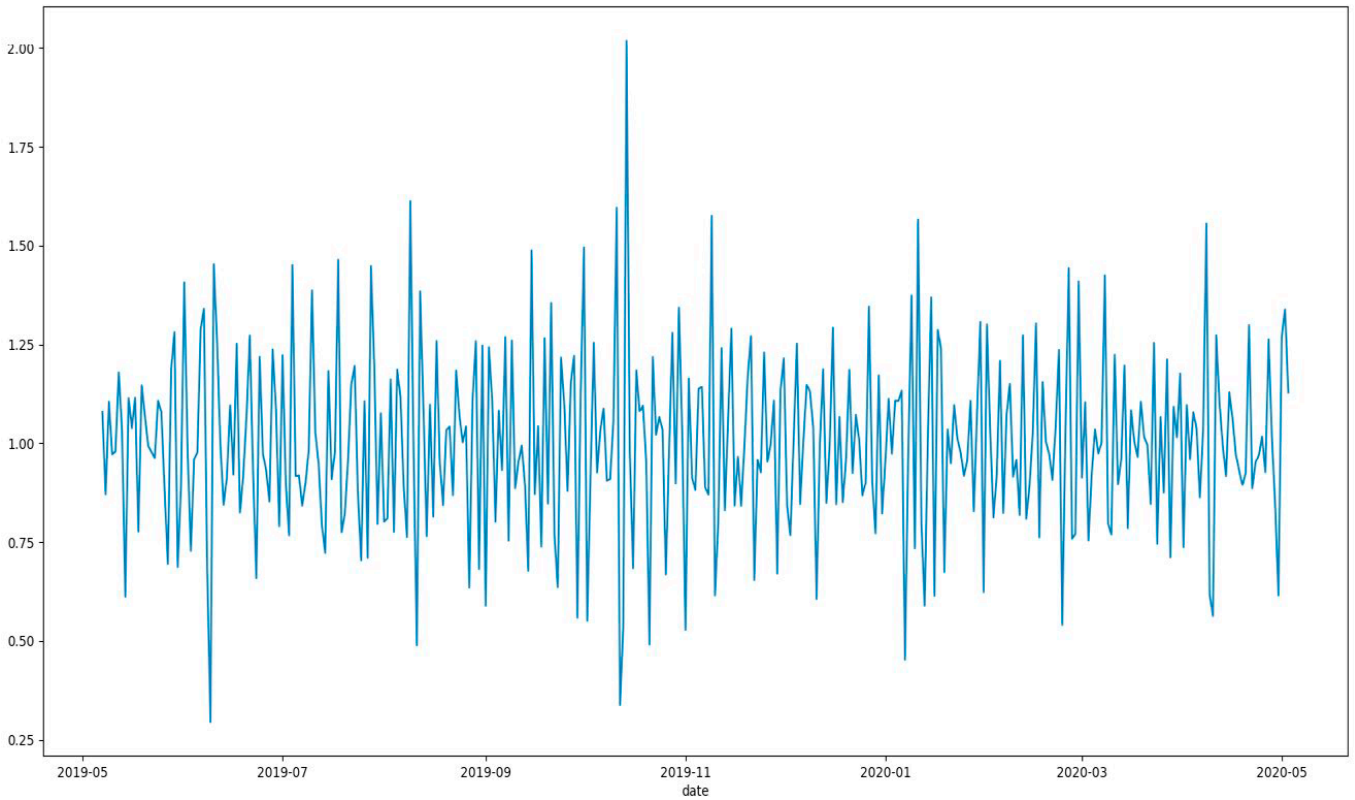

Figure 3. A relative activity graph example of the far-right VKontakte community.

For reliable identification of the group, the rise in, high level, and decline of activity in the group were recorded on different dates (representing the calendar of key events, the knowledge base). For example, the activity increased significantly in the vicinity of "20.04", which is a day significant for the far-right because it is associated with a specific character. Another example is the increase of activity around "16.10", which is the date of the founding of the RNE (Russian far-right nationalist organization). A further example of this is with the birthdates "09.06" and "17.10". It is worth noting that "staples" in dates in far-right communities show how the activity intensifies. The "demiurges" of the far-right communities constantly search for meaningful "staples" to fund the activity. Activists set the ideological agenda, allowing users to demonstrate their connection to the movement. Figure 4 presents an EPC diagram reflecting the mechanism of the method and its relationship to the software elements for an automated search of far-right communities (Vilnin et al. 2021).

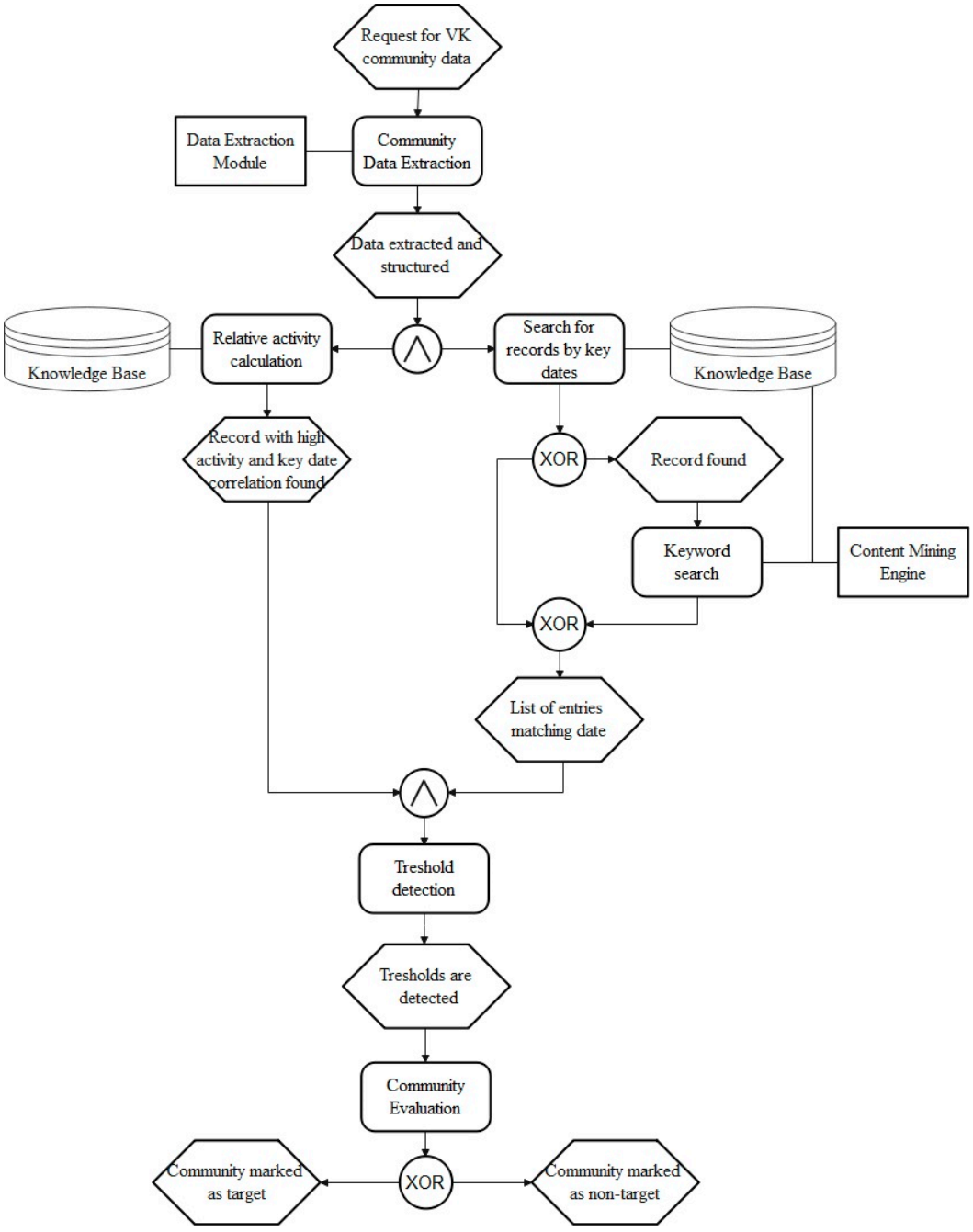

Figure 4. EPC diagram of the CCA algorithm.

It is worth noting the main limiting factors in using the CCA algorithm.

First, the method is highly demanding in terms of the knowledge base quality that describes dates and related keywords relevant to far-right ideological platforms. The information in the knowledge base requires constant updating for the method to work effectively. Second, the method is not sensitive to the tone of content published in the online community, leading to false-positive results because significant individual dates can also provoke activity in opposition to far-right communities as they are informative occasions. Third, it is impractical to check each community individually given that their total number is in the tens of millions. Thus, CCA can only be used as an additional tool when we already have a single VKontakte-community in our "field of view". In generalized form, the automated search for far-right communities using the CCA boils down to the following sequence of actions (Figure 5):

(a) The expert user builds a "knowledge base" (a list of keywords, expressions, and dates, including defining their relationships);
(b) The user launches the primary keyword search function;
(c) Pre-processing of the results (deleting closed, inactive, "empty" communities);
(d) The method of calendar-correlation analysis is used to refine the list of identified far-right communities;
(e) The expert analyzes the results and enters them into the knowledge base, if necessary;
(f) The user builds a set of groups for further search of related communities (satellites);
(g) The results of the search for the satellite communities are analyzed. If necessary, the expert refines the information in the knowledge base.

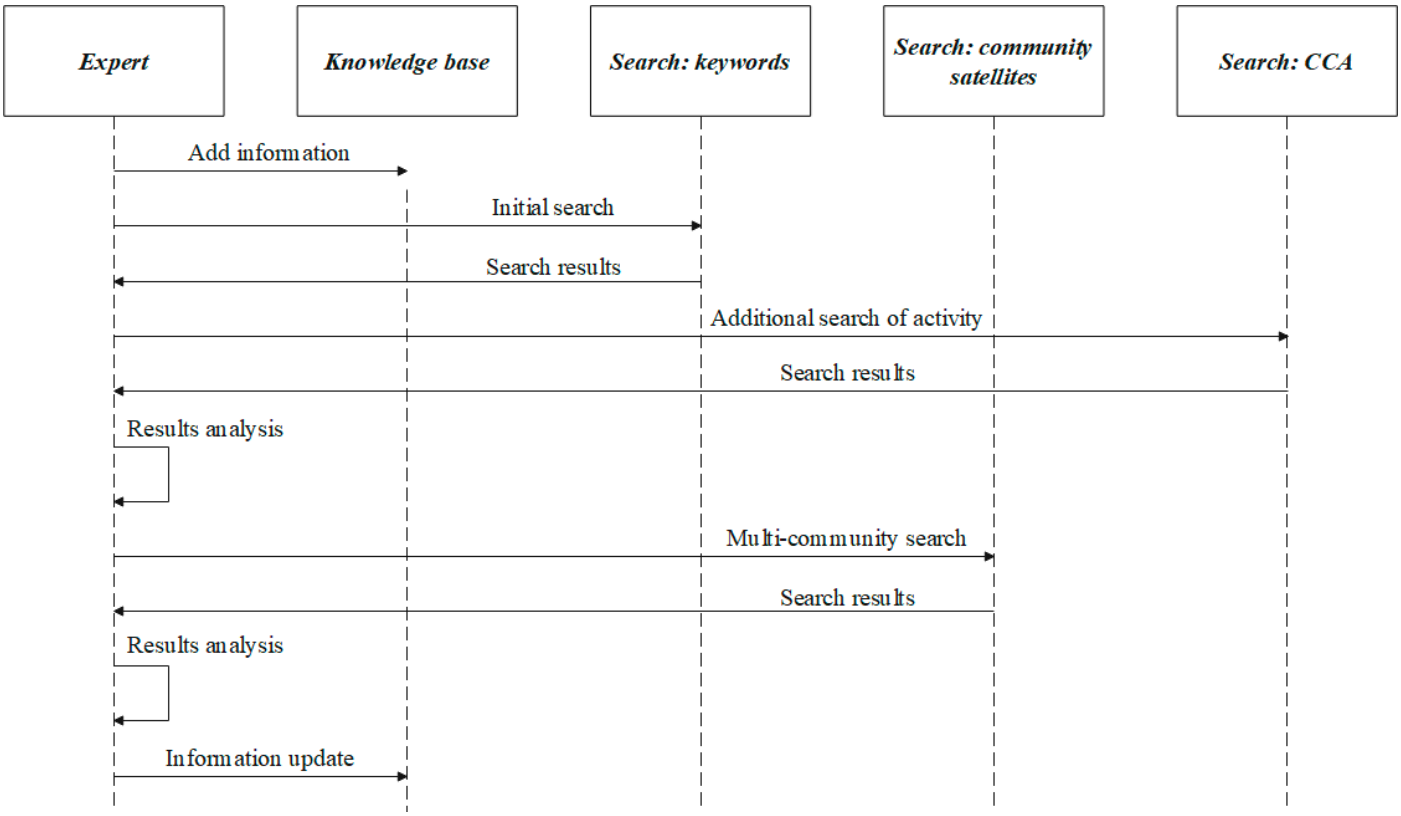

Figure 5. Sequence diagram of the generalized algorithm for detecting active far-right ideological platforms in social media and information influence from the far-right ideological platform.

5. Experimental Testing of CCA and Results Discussion

We evaluated the effectiveness of the CCA method on two datasets. The first dataset was expertly generated and included VKontakte communities belonging to various far-

right ideological platforms. The first dataset included 259 entries. The second dataset included 49 of the most popular VKontakte communities and was formed based on the social network's statistics. The expert reviewed the communities in the second dataset and did not classify them as having features of a far-right ideological platform.

The experimental study automatically tested each community in the dataset against two mutually exclusive hypotheses.

Hypothesis 0 (H0). *The Vkontakte community does not contain signs of belonging to a far-right ideological platform.*

Hypothesis 1 (H1). *The VKontakte community exhibits signs of belonging to a far-right platform.*

On the first set of data, hypothesis H0 was erroneously accepted in 210 cases. Correspondingly, hypothesis H1 was correctly accepted in 49 cases. Thus, the probability of type II error was $\beta = 0.81$ and the power of the criterion $(1 - \beta) = 0.19$.

As part of testing the CCA algorithm on the second set of data, hypothesis H1 was erroneously accepted in one case. Consequently, the probability of type I error was 0.02.

The analysis of the experimental test results showed that the current version of the knowledge base contains mainly information about significant events and dates in the history of the Third Reich. At the same time, the first dataset includes communities belonging to such far-right subclasses as alt-right, Nazis, neo-pagans, manosphere, and communities without a clear ideological orientation (designated as "far-right"). The magnitudes of type II errors relative to the subclasses were recalculated and Table 1 presents the corresponding results.

Table 1. Type II error and criterion power for different subclasses.

Subclass	β	$1 - \beta$	Number of Communities within the Dataset
Alt-Right	0.67	0.33	6
Nazis	0.5	0.5	12
Neo-Pagans	0.91	0.09	67
Manosphere	0.95	0.05	19
Far-Right	0.78	0.22	155

We interpreted the relatively low accuracy of the algorithm as the result of incomplete information provided in the knowledge base. Additionally, the fact that, for specific subclasses of the far-right ideological platform, the accuracy of the CCA was higher confirms our thesis. Thus, we can conclude that different communities respond to and honor different dates and related keywords, and greater accuracy can be achieved by refining the existing knowledge base and developing rules to populate and maintain it. Table 2 provides background information on VKontakte communities automatically categorized as having signs of belonging to a far-right ideological platform. During the preparation of statistics, 4 out of 49 communities denied access to information about themselves, so the table shows only 45 communities.

In the VKontakte social network, the user must specify a value in the column "Gender". The default value when registering a new account is "male". Thus, if the user's profile gender is «male», it can also be interpreted as a reluctance of the user to specify gender.

Table 2. Background information on the communities detected by the CCA.

№	Subscribers	Age			Gender, %		Posts	
		Median	Average	Not Specified, %	Male	Female	Over the Year	Daily Average
1	735,113	26	29.94	66.49%	50.20%	49.80%	9195	24.71
2	293,537	31	33.57	66.27%	66.24%	33.76%	2336	6.27
3	89,134	21	27.97	62.34%	28.24%	71.76%	1786	4.80
4	20,485	32	35.67	66.49%	87.68%	12.32%	110	0.29
5	17,828	33	37.85	65.61%	82.89%	17.11%	5152	13.85
6	17,281	35	39.05	61.77%	82.10%	17.90%	1944	5.22
7	28,999	22	33.09	57.56%	90.67%	9.33%	2323	6.24
8	8792	36	39.67	62.82%	79.80%	20.20%	1324	3.55
9	10,215	26	33.13	61.82%	85.16%	14.84%	1947	5.23
10	6590	25	36.74	61.96%	88.98%	11.02%	316	0.84
11	6317	34	39.5	70.06%	85.88%	14.12%	62	0.16
12	3516	34	38.66	74.29%	85.86%	14.14%	18	0.04
13	5985	23	34.3	57.59%	90.69%	9.31%	712	1.91
14	4066	28	37.23	61.78%	87.16%	12.84%	45	0.12
15	1344	40	43.53	55.06%	84.15%	15.85%	236	0.63
16	8673	34	38.79	66.67%	86.15%	13.85%	469	1.25
17	7233	25	33.98	58.72%	83.49%	16.51%	416	1.11
18	14,591	33	37.55	62.99%	82.75%	17.25%	180	0.48
19	9433	36	39.97	60.03%	87.33%	12.67%	589	1.58
20	47,652	25	31.92	56.64%	75.67%	24.33%	2013	5.41
21	1155	36	39.39	57.14%	62.77%	37.23%	830	2.23
22	16,448	35	39.03	53.34%	86.89%	13.11%	37	0.09
23	3300	37	40.84	68.06%	74.64%	25.36%	2629	7.06
24	24,219	33	37.87	59.81%	85.05%	14.95%	1765	4.74
25	80,236	37	39.51	60.67%	76.04%	23.96%	3221	8.65
26	85,574	36	39.35	67.74%	62.59%	37.41%	2002	5.38
27	60,125	38	40.89	61.59%	63.00%	37.00%	3143	8.44
28	80,484	38	40.92	61.91%	65.92%	34.08%	4669	12.55
29	66,489	32	35.14	64.36%	72.40%	27.60%	807	2.16
30	21,209	31	34.81	64.35%	80.81%	19.19%	28	0.07
31	576	33	36.09	77.95%	52.60%	47.40%	575	1.54
32	50,355	38	41.99	63.22%	69.00%	31.00%	3016	8.10
33	245,091	39	41.06	63.18%	45.70%	54.30%	5487	14.74
34	63,106	33	34.89	71.78%	55.35%	44.65%	933	2.50
35	58,156	24	27.45	50.95%	59.78%	40.22%	5171	13.90
36	4543	32	38.1	57.45%	85.41%	14.59%	724	1.94
37	9850	35	39.51	68.36%	81.40%	18.60%	439	1.18
38	3054	21	35.59	54.78%	86.25%	13.75%	171	0,45
39	4114	29	36.76	53.33%	83.50%	16.50%	323	0.86
40	51,149	37	40.41	61.50%	80.78%	19.22%	6942	18.66
41	30,091	20	32.87	55.24%	79.85%	20.15%	807	2.16
42	18,017	22	32.91	54.00%	89.09%	10.91%	6728	18.08
43	19,634	36	39.53	59.88%	57.57%	42.43%	2134	5.73
44	51,204	39	41.34	55.77%	63.79%	36.21%	4921	13.22

45	143,657	39	41.61	66.19%	42.87%	57.13%	744	2

One of the main problems in the automation of sociological and political science research using social network data is the high labor intensity of the initial process of searching for far-right communities. The CCA algorithm reduces the laboriousness of the initial stage of the work, and researchers can apply it at the preliminary stage for researching online radicalization processes in social media. Experimental testing of the algorithm was carried out only for the texts in Russian. It is possible to extend the CCA approach for the analysis of texts in other languages, provided that the knowledge base includes a description of key dates and related events in the target languages.

6. Conclusions

For experts, far-right violence represents a significant problem and concern as a growing threat, particularly as the ideological, financial, organizational, and transnational ties of far-right extremist communities are consolidated internationally. The expert community does not yet understand the emerging trend that is the reaction to the crisis associated with the coronavirus pandemic. COVID-19 has created a new source of anger and discontent among some of the world's population. However, most dangerously, it is a new trigger for future episodes of domestic far-right terrorism against targets symbolizing personal grievances and projected into political discontent on racist, anti-immigration, anti-government, and other grounds. The far-right is already trying to use the "infodemic" (information epidemic) by spreading misinformation and fake news, by creating and promoting conspiracy theories, by the use of trolling, cyberbullying, and doxing on social networks, thus, accelerating the polarization of the population and inciting violent actions. The relevance of creating tools for identifying information epidemics on social media is thus growing alongside these threats. One cannot exclude such a growing threat as large-scale attacks by lone actors or autonomous cells under the influence of pandemic crisis conspiracies. Consequently, there is a need for efficient monitoring of social networks to predict and defend the likely targets of such attacks as well as to better understand the dynamics of far-right communities for academic research.

The speed and reliability of computer-based analytical methods in creating tools for research on online radicalization on social networks depend directly on the quality of (1) the formalization of variables by an expert covering subjective meaning and content that computer software can detect; (2) the presentation of unstructured data in a form suitable for subsequent algorithmic research tasks; (3) the classification and clustering of far-right ideologies and terrorist crimes committed on the basis of those ideologies, and differentiating them from those that may be weaker and potentially categorized as non-ideologically motivated hate crimes; and (4) the identification of clear indicators.

Research teams working on the prototyping of such computer-based analytical methods have to deal with organizing an effective mechanism for extracting raw data when automating online radicalization research. The primary tool for this is using APIs provided by social network owners. The user agreement limits the use of APIs, which usually limits the amount of content provided in response to a request. In international practice, there are already examples when research centres and teams working in social mining fields are provided with special conditions of API use (for example, increased limits for information extraction, additional "fields" of data, and others) to improve the quality of research results.

The presented CCA algorithm for detection of far-right extremist communities allows identifying such communities with high accuracy and is applicable to studies of the process of online radicalization in a social network. Moreover, the developed prototype can be adjusted (under the condition of dataset supplementation) not only for far-right extremist communities but also for revealing school shooters, as this group is also "sensitive" to dates and events. In the future, one can adjust this approach to the analysis of

other social networks, subject to the expansion of the "knowledge base" and adaptation to the API of social network.

The accuracy of CCA depends directly on the accuracy of the data in the knowledge base describing dates and personalities significant to the ideological platform. With appropriate changes in the knowledge base, it is possible to search not only far-right communities. Additionally, the proposed approach is applicable to any social media that allows the automatic retrieval of the date of posted content. Filling the knowledge base with information on other ideological platforms, among other things, will allow studying the nature and strength of their interrelations and mutual influence. The use of CCA (provided that the knowledge base is populated) can effectively identify loners (category: school shooters, mass murderers, and lone-wolf terrorists) who have a high degree of radicalization and risk of committing incidents. For this category of radicals, "staples" such as honoring dates, events, and heroic figures are essential.

Author Contributions: Conceptualization, A.K.; methodology, A.K.; data curation, A.S.; software, A.V. and S.K.; writing—original draft preparation, A.K.; writing—review and editing, A.K. and A.S.; formal analysis, A.V.; visualization, A.S. and A.V.; investigation, S.K.; supervision, A.K.; project administration, A.K.; funding acquisition, A.K; validation, A.K. and S.K.; resources, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Ministry of Science and Higher Education of the Russian Federation as a part of the project No. FSWW 2020–0014.

Data Availability Statement: The data are available upon request from the corresponding authors.

Conflicts of Interest: The authors declare no conflict of interest.

References

(AIVD 2019) AIVD. 2019. AIVD-Jaarverslag 2019. Available online: https://www.aivd.nl/documenten/jaarverslagen/2020/04/29/jaarverslag-2019 (accessed on 15 March 2022).

(Anderson 2012) Anderson, Chris. 2012. Towards a sociology of computational and algorithmic journalism. *New Media & Society* 15: 1005–21. https://doi.org/10.1177/1461444812465137.

(Barhamgi et al. 2018) Barhamgi, Mahmoud, Abir Masmoudi, Raul Lara-Cabrera, and David Camacho. 2018. Social networks data analysis with semantics: Application to the radicalization problem. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-018-0968-z. Available online: https://link.springer.com/article/10.1007/s12652-018-0968-z (accessed on 15 March 2022).

(Bjørgo and Ravndal 2019) Bjørgo, Tore, and Jacob A. Ravndal. 2019. Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses. ICCT. Available online: https://icct.nl/app/uploads/2019/09/Extreme-Right-Violence-and-Terrorism-Concepts-Patterns-and-Responses.pdf (accessed on 15 March 2022).

(Borum 2004) Borum, Randy. 2004. Psychology of Terrorism. Office of Justice Programs. Available online: https://www.ojp.gov/sites/g/files/xyckuh241/files/media/document/208552.pdf?height=921.6&q=psychology-of-terrorism%3FTB_iframe%3Dtrue&width=921.6 (accessed on 15 March 2022).

(Borum 2011) Borum, Randy. 2011. Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security* 4: 7–36. https://doi.org/10.5038/1944-0472.4.4.1.

(Botometer 2021) Botometer. 2021. Botometer an OSoMe Project. Available online: https://botometer.osome.iu.edu (accessed on 15 March 2022).

(Braniff 2017) Braniff, William. 2017. Recasting and Repositioning CVE as a Grand Strategic Response to Terrorism. START. Available online: https://www.start.umd.edu/news/recasting-and-repositioning-cve-grand-strategic-response-terrorism (accessed on 15 March 2022).

(Cherniy 2021) Cherniy, Vasilii. 2021. Social Networks in Russia: Figures and Trends, Fall 2021. Brand Analytics. Available online: https://br-analytics.ru/blog/social-media-russia-2021/ (accessed on 15 March 2022).

(Conway 2017) Conway, Maura. 2017. Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism* 40: 77–98. https://doi.org/10.1080/1057610X.2016.1157408.

(Forelle et al. 2015) Forelle, Michelle, Phil Howard, Andrés Monroy-Hernández, and Saiph Savage. 2015. Political Bots and the Manipulation of Public Opinion in Venezuela. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2635800 (accessed on 15 March 2022).

(Garcet 2021) Garcet, Serge. 2021. Understanding the psychological aspects of the radicalisation process: A sociocognitive approach, Forensic Sciences Research. doi:10.1080/20961790.2020.1869883. Available online: https://www.tandfonline.com/doi/full/10.1080/20961790.2020.1869883.pdf (accessed on 15 March 2022).

(Gaudette et al. 2020) Gaudette, Tiana, Ryan Scrivens, and Vivek Venkatesh. 2020. The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists, Terrorism and Political Violence. *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2020.1784147. Available online: https://www.tandfonline.com/doi/full/10.1080/09546553.2020.1784147?scroll=top&needAccess=true (accessed on 15 March 2022).

(Gilani et al. 2017) Gilani, Zafar, Ekaterina Kochmar, and Jon Crowcroft. 2017. Classification of Twitter Accounts into Automated Agents and Human Users. Paper present at the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). Sydney, Australia, July 3–August 3. https://doi.org/10.1145/3110025.3110091.

(Golikov 2021) Golikov, Leonid. 2021. Utilitarian Necessity and Desire in the Russian Nationalist Discourse (Based on the Content from VKontakte Social Group "Sputnik i Pogrom"). Available online: https://www.gramota.net/articles/phil210511.pdf (accessed on 15 March 2022).

(GTI 2019) GTI. 2019. Global Terrorism Index 2019. Available online: https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2019-web.pdf (accessed on 15 March 2022).

(GTI 2020) GTI. 2020. Global Terrorism Index 2020. Available online: https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf (accessed on 15 March 2022).

(Hall et al. 2019) Hall, Margeret, Michael Logan, Gina S. Ligon, and Douglas C. Derrick. 2019. Do Machines Replicate Humans? Toward a Unified Understanding of Radicalizing Content on the Open Social Web. *Policy & Internet* 12: 109–38. https://doi.org/10.1002/poi3.223.

(Hamm and Spaaij 2015) Hamm, Mark, and Ramon Spaaij. 2015. Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies. Available online: https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf (accessed on 15 March 2022).

(Hashemi and Hall 2019) Hashemi, Mahdi, and Margeret Hall. 2019. Detecting and Classifying Online Dark Visual Propaganda. *Image and Vision Computing* 89: 95–105. https://doi.org/10.1016/j.imavis.2019.06.001.

(Heide et al. 2018) Heide, Liesbeth, Charlie Winter, and Shiraz Maher. 2018. The Cost of Crying Victory: Policy Implications of the Islamic State's Territorial Collapse. ICCT. Available online: https://icsr.info/wp-content/uploads/2019/01/ICSR-ICCT-Feature_The-Cost-of-Crying-Victory-Policy-Implications-of-the-Islamic-State's-Territorial-Collapse.pdf (accessed on 15 March 2022).

(Hofmann 2018) Hofmann, David C. 2018. How "Alone" are Lone-Actors? Exploring the Ideological, Signaling, and Support Networks of Lone-Actor Terrorists. *Journal Studies in Conflict & Terrorism* 43: 657–78. https://doi.org/10.1080/1057610X.2018.1493833.

(Holt et al. 2020) Holt, Thomas J., Joshua D. Freilich, and Steven M. Chermak. 2020. Examining the Online Expression of Ideology among Far-Right Extremist Forum Users. *Terrorism and Political Violence* 34: 364–84 https://doi.org/10.1080/09546553.2019.1701446.

(Jasser et al. 2020) Jasser, Greta, Megan Kelly, and Ann-Kathrin Rothermel. 2020. Male Supremacism and the Hanau Terrorist Attack: Between Online Misogyny and Extreme Right Violence. ICCT. Available online: https://icct.nl/publication/male-supremacism-and-the-hanau-terrorist-attack-between-online-misogyny-and-far-right-violence/ (accessed on 15 March 2022).

(Jensen et al. 2018) Jensen, Michael A., Anita A. Seate, and Patrick A. James. 2018. Radicalization to Violence: A Pathway Approach to Studying Extremism. *Terrorism and Political Violence* 32: 1067–90. https://doi.org/10.1080/09546553.2018.1442330.

(Johnson 2021) Johnson, Joseph. 2021. Global Digital Population as of January 2021. Statista. Available online: https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed on 15 March 2022).

(Karpova et al. 2019) Karpova, Anna Yu, Aleksei O. Savelev, Alexandr D. Vilnin, and Denis V. Chaykovskiy. 2019. New technologies to identify alt-right extremist communities in social media. Vestnik tomskogo gosudarstvennogo universi-teta-filosofiya-sotsiologiya-politologiya-tomsk state. *University Journal of Philosophy Sociology and political Science* 52: 138–46. https://doi.org/10.17223/1998863X/52/14.

(Karpova et al. 2020) Karpova, Anna Yu, Aleksei O. Savelev, Alexandr D. Vilnin, and Denis V. Chaykovskiy. 2020. Studying Online Radicalization of Youth through Social Media (Interdisciplinary Approach). *Monitoring of Public Opinion: Economic and Social Changes* 3: 159–81. https://doi.org/10.14515/monitoring.2020.3.1585.

(Kozitsin et al. 2020) Kozitsin, Ivan, Alexander Chkhartishvili, Artemii Marchenko, Dmitrii Norkin, Sergei Osipov, Ivan Uteshev, Vyacheslav Goiko, Roman Palkin, and Michail Myagkov. 2020. Modeling Political Preferences of Russian Users Exemplified by the Social Network Vkontakte. *Math Models Comput Simul* 12: 185–94. https://doi.org/10.1134/S2070048220020088.

(Kutner 2020) Kutner, Samantha. 2020. Swiping Right: The Allure of hYper Masculinity and Cryptofascism for Men Who Join the Proud Boys. ICCT. Available online: https://icct.nl/app/uploads/2020/05/Swiping-Right-The-Allure-of-Hyper-Masculinity-and-Cryptofascism-for-Men-Who-Join-the-Proud-Boys.pdf (accessed on 15 March 2022).

(Kuznetsov et al. 2021) Kuznetsov, Sergei A., Anna Yu Karpova, and Aleksei O. Savelev. 2021. Automated detection of ultra-right communities' cross-links in a social network. Vestnik tomskogo gosudarstvennogo universiteta-filosofiya-sotsiologiya-politologiya-tomsk state univer-sity. *Journal of Philosophy Sociology and Political Science* 59: 156–66. 10.17223/1998863X/59/15.

(LaFree 2013) LaFree, Gary. 2013. Lone-Offender Terrorists. *Criminology and Public Policy* 12: 59–62. https://doi.org/10.1111/1745-9133.12018.

(Lewis 2018) Lewis, Rebecca. 2018. Alternative Influence: Broadcasting the Reactionary Right on YouTube. Available online: https://datasociety.net/wp-content/uploads/2018/09/DS_Alternative_Influence.pdf (accessed on 15 March 2022).

(McCauley and Moskalenko 2008) McCauley, Clark, and Sophia Moskalenko. 2008. Mechanisms of political radicalisation: Pathways toward terrorism. *Terrorism and Political Violence* 20: 415–33. https://doi.org/10.1080/09546550802073367.

(McCauley and Moskalenko 2017) McCauley, Clark, and Sophia Moskalenko. 2017. Understanding political radicalization: The two-pyramids model. *American Psychologist* 72: 205–16. https://doi.org/10.1037/amp0000062.

(Minjust 2021) Minjust. 2021. The Ministry of Justice of the Russian Federation Federal List of Extremist Materials. Available online: https://minjust.gov.ru/ru/extremist-materials/ (accessed on 15 March 2022).

(MSC 2020) MSC. 2020. Munich Security Report 2020. Available online: https://securityconference.org/assets/user_upload/MunichSecurityReport2020.pdf (accessed on 15 March 2022).

(NAC 2021) NAC. 2021. List of Public and Religious Associations, and Other Non-Profit Organizations. Available online: http://nac.gov.ru/zakonodatelstvo/sudebnye-resheniya/perechen-nekommercheskih-organizaciy-v.html (accessed on 15 March 2022).

(Neumann 2009) Neumann, Peter R. 2009. Old and New Terrorism. Cambridge: Polity Press. Available online: https://www.wiley.com/en-us/Old+and+New+Terrorism-p-9780745643755 (accessed on 15 March 2022).

(Pipiya 2019) Pipiya, Karina. 2019. Monitoring xenophobic attitudes. Available online: https://bit.ly/3xJFpHN (accessed on 15 March 2022).

(Poupin 2021) Poupin, Perrine. 2021. Social media and state repression: The case of VKontakte and the anti-garbage protest in Shies, in Far Northern Russia. *First Monday* 26. https://doi.org/10.5210/fm.v26i5.11711. Available online: https://journals.uic.edu/ojs/index.php/fm/article/view/11711 (accessed on 15 March 2022).

(PST 2020) PST. 2020. Nasjonal Trusselvurdering. Available online: https://www.pst.no/globalassets/artikler/utgivelser/2020/nasjonal-trusselvurdering-2020-print.pdf (accessed on 15 March 2022).

(Rahwana et al. 2020) Rahwana, Iyad, Jacob W. Crandall, and Jean-Francois Bonnefon. 2020. Intelligent machines as social catalysts. *Proceedings of the National Academy of Sciences* 117: 7555–57. https://doi.org/10.1073/pnas.2002744117.

(Ravndal and Bjørgo 2018) Ravndal, Jacob A., and Tore Bjørgo. 2018. Investigating Terrorism from the Extreme Right: A Review of Past and Present Research. *Perspectives on Terrorism* 12: 5–22. Available online: https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2018/issue-6/a1-ravndal-and-bjorgo.pdf (accessed on 15 March 2022).

(Reuter and Szakonyi 2015) Reuter, Ora, and David Szakonyi. 2015. Online social media and political awareness in authoritarian regimes. *British Journal of Political Science* 45: 29–51. https://doi.org/10.1017/S0007123413000203.

(Sanovich et al. 2018) Sanovich, Sergey, Denis Stukal, and Joshua A. Tucker. 2018. Turning the virtual tables: Government strategies for addressing online opposition with an application to Russia. *Comparative Politics* 50: 435–82. https://doi.org/10.5129/001041518822704890.

(Savelev et al. 2021) Savelev, Aleksei O., Anna Yu Karpova, Denis V. Chaykovskiy, Alexandr D. Vilnin, Anastasia Yu Kaida, Sergei A. Kuznetsov, Lev O. Igumnov, and Nataliya G. Maksimova. 2021. The high-level overview of social media content search engine. *IOP Conference Series: Materials Science and Engineering* 1019: 012097. https://doi.org/10.1088/1757-899X/1019/1/012097.

(Siebel 2019) Siebel, Thomas M. 2019. *Digital Transformation: Survive and Thrive in an Era of Mass Extinction*. New York: RosettaBooks.

(Statista Research Department 2022) Statista Research Department. 2022. Social media—Statistics & Facts. Statista. January. Available online: https://www.statista.com/topics/1164/social-networks/#topicHeader__wrapper (accessed on 15 March 2022).

(Stella et al. 2018) Stella, Massimo, Emilio Ferrara, and Manlio De Domenico. 2018. Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems. Available online: https://www.pnas.org/content/115/49/12435 (accessed on 15 March 2022).

(Stieglitz et al. 2018) Stieglitz, Stefan, Milad Mirbabaie, Björn Ross, and Christoph Neuberger. 2018. Social media analytics—Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management* 39: 156—68. https://doi.org/10.1016/j. ijinfomgt.2017.12.002.

(Sureka and Agarwal 2014) Sureka, Ashish, and Swati Agarwal. 2014. Learning to classify hate and extremism promoting tweets. Paper present at the 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, The Netherlands, September 24–26. https://doi.org/10.1109/JISIC.2014.65.

(Tang and Liu 2010) Tang, Lei, and Huan Liu. 2010. Community Detection and Mining in Social Media. In *Synthesis Lectures on Data Mining and Knowledge Discovery*. Morgan & Claypool. https://doi.org/10.2200/S00298ED1V01Y201009DMK003. Available online: https://www.morganclaypool.com/doi/abs/10.2200/S00298ED1V01Y201009DMK003 (accessed on 15 March 2022).

(Turner 2011) Turner, Matthew D. 2011. A Simple Ontology for the Analysis of Terrorist Attacks. Technical Report. Available online: https://digitalrepository.unm.edu/ece_rpts/41/ (accessed on 15 March 2022).

(Urman 2019) Urman, Aleksandra. 2019. News Consumption of Russian Vkontakte Users: Polarization and News Avoidance. *International Journal of Communication* 13: 5158–82.

(Varol et al. 2017) Varol, Onur, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, and Alessandro Flammini. 2017. Online Human-Bot Interactions: Detection, Estimation, and Characterization. Paper present at the International AAAI Conference on Web and Social Media, Montreal, QC, Canada, May 15–18. Available online: https://arxiv.org/pdf/1703.03107.pdf (accessed on 15 March 2022).

(Vilnin et al. 2021) Vilnin, Alexandr D., Anastasia Yu Kaida, Anna Yu Karpova, Sergei A. Kuznetsov, Nataliya G. Maksimova, Aleksei O. Savelev, and Denis V. Chaykovskiy. 2021. Calendar-Correlation Analysis of the Activity of Social Network Communities. Certificate of State Registration of the Computer Program 2021662860 Dated 6 August 2021. Available online: https://elibrary.ru/download/elibrary_46484745_77252480.PDF (accessed on 15 March 2022).

(Wadhwa and Bhatia 2013) Wadhwa, Pooja, and M. P. S. Bhatia. 2013. Tracking on-line radicalization using investigative data mining. Paper present at the 2013 National Conference on Communications (NCC), New Delhi, India, February 15–17. https://doi.org/10.1109/NCC.2013.6488046.

(Weiler et al. 2016) Weiler, Andreas, Michael Grossniklaus, and Marc H. Scholl. 2016. Situation monitoring of urban areas using social media data streams. *Information Systems* 57: 129–41. https://doi.org/10.1016/j.is.2015.09.004.

(Wendelberg 2021) Wendelberg, Linda. 2021. An Ontological Framework to Facilitate Early Detection of 'Radicalization' (OFEDR)-A Three World Perspective. *Journal of Imaging* 7: 60. https://doi.org/10.3390/jimaging7030060.

(Whiting et al. 2021) Whiting, Tim, Alvika Gautam, Jacob Tye, Michael Simmons, Jordan Henstrom, Mayada Oudah, and Jacob W. Crandall. 2021. Confronting barriers to human-robot cooperation: Balancing efficiency and risk in machine behavior. *iScience* 24: 101963. https://doi.org/10.1016/j.isci.2020.101963.

(Xie et al. 2016) Xie, Daniel, Xu Jiejun, and Tsai-Ching Lu. 2016. Automated Classification of Extremist Twitter Accounts Using Content-Based and Network-Based Features. Paper present at the 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, December 5–8. 10.1109/BigData.2016.7840895.

(Yudina 2020) Yudina, Natalia. 2020. Report: Ultra-Right Criminal Activity. Hate Crimes and Countering Them in Russia in 2019. Available online: https://bit.ly/3jVHvMJ (accessed on 15 March 2022).