No. 282 12 April 2022

russian analytical digest

www.css.ethz.ch/en/publications/rad.html

RUSSIAN INFORMATION WARFARE

German Association for
East European Studies

Institute for European,
Russian, and Eurasian Studies
The George Washington
University

Research Centre
for East European Studies
University of Bremen

Center for
Security Studies
ETH Zurich

Center for
Eastern European Studies
University of Zurich

INTRODUCTION

Russia's Information Warfare

This issue of the *Russian Analytical Digest* features a series of articles examining Russian information warfare. Over the past decade, Vladimir Putin's Russia has employed unorthodox foreign policy tools with increasing frequency, intensity, and success. Perhaps the most effective of these tactics has been the use of information warfare designed to affect decision-making in countries Russia considers to be its adversaries. In the target countries, these measures aim to destabilize civil society, erode trust in democratic institutions, and foster uncertainty among allies.

If the United States and Europe hope to defend their economies, institutions, and identities, an immediate and effective policy response is required. To date, however, the United States and many of its European partners have struggled to develop policies that combat and counter Russian information warfare.

The articles gathered here examine the tools that Russia has used against Ukraine, Poland, the United States, and the European Union, as well as the strategies that these countries have employed to combat Russian information warfare. The joint article by the four authors concisely summarizes the findings and proposes policy options by means of which the democratic countries of the West can address the challenges information warfare poses. The final article looks at Russia, examining controversies around the political role of the aggregator Yandex.news in prioritizing media news.

ANALYSIS

Adaptive Russian Information Warfare in Ukraine

By Nash Miller (George Washington University)

DOI: 10.3929/ethz-b-000541999

Abstract

Information warfare is a key component of Russia's national security strategy and has impacted the United States, Europe, and—perhaps most notably—Ukraine. Ukraine has been on the front lines of Russia's information war for a decade, with Russia using both traditional mass media and social media to create divisions within the country and justify war. Ukrainian responses have involved limitations and bans on Russian mass media, attempts to expose Russian misinformation, and information campaigns of its own. These policy responses have forced Russian tools to adapt and have limited the audience of Russian information warfare.

Russian Tools

Perhaps nowhere is Russian information warfare more clearly on display than in Ukraine. Since before the 2014 Euromaidan Revolution, information campaigns have been a staple of Russian strategy in the country, being used to leverage ethno-linguistic cleavages, sow confusion and distrust, and fabricate justifications for war. This analysis will identify Russian tools and strategies of information warfare in Ukraine since 2014 and lay out Ukrainian policy responses.

Current Russian information warfare is an outgrowth of Soviet-era "active measures" and a key component of today's much-discussed Gerasimov Doctrine, or "hybrid warfare," which seemingly dominates Russian strategy. Russia employs many tools to wage its information warfare, including directly controlled state media, indirect control of traditional media (*samodeitelnost*), and social media efforts.

The Kremlin exercises direct control over many of the largest media outlets in Russia, which also broadcast throughout the former Soviet Union, including Ukraine. Each week, representatives of large Russian television channels, including Pervyi Kanal, NTV, Rossiia 1, and others, meet with Kremlin officials to receive approved narratives. Multiple pro-Kremlin Ukrainian channels are also said to have direct connections with Putin's inner circle. In 2014, 97% of Ukrainians reported that television was their main source of news, a share much higher than in other European countries (Onuch, 2021, p. 3). During the run-up to and immediate aftermath of the Euromaidan Revolution, Russian or Russian-controlled television enjoyed dominant viewership throughout Ukraine.

But the Kremlin also controls other media indirectly through a phenomenon known as *samodeitelnost*, or "independent initiative." Due to a combination of motivating carrots and threatening sticks, independent journalists, media outlets, and social media creators produce and disseminate information content that they anticipate will be in line with the Kremlin's desires.

Russia's innovative use of social media as a tool of information warfare has also had a major impact. Several pro-Kremlin Telegram channels in Ukraine—such as WarGonzo, Ukraine.Ru, and Donbass Decides—have over half a million subscribers apiece. Content from such channels is shared and re-shared across multiple social media platforms, flooding feeds with pro-Russian narratives. Often, content from these local pro-Russian Telegram channels in Ukraine eventually makes its way onto one of the main television channels in Russia.

Russian Information Strategy after Euromaidan

Russian messaging can be incredibly flexible to accomplish its aims and can pursue multiple contradictory narratives at once to sow confusion and fear. Russian information campaigns following the Euromaidan Revolution in 2014 focused on exploiting existing ethnolinguistic cleavages in Ukraine to spread existential fear among Russophones in the country.

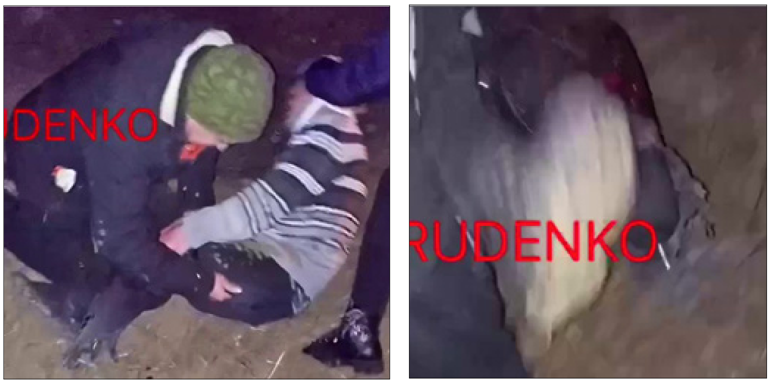
Highlighting the collaboration of some Ukrainian nationalists with the Nazi occupiers during the Second World War, Russian media was swift to label Euromaidan protestors and the resulting new government as "fascists" (Osipian, 2015, p. 152) and "brutal Russophobic thugs" (Osipian, 2015, p. 119). Multiple Russian-language television channels declared that soon, neo-Nazis from Western Ukraine would come to Crimea and the Donbass to carry out genocidal reprisals against Russophones. Russian media couched the conflict in the Donbass in the language of the Great Patriotic War, using terms like "Banderists," "fascist," "Nazi," "*opolchentsy*" (defensive militia created during wartime), and "anti-fascist" to depict the combatants on the two sides. Russian media expertly instrumentalized powerful historical memories of the Great Patriotic War to paint the new regime in Kyiv as an existential threat to Russian-speakers in Ukraine.

As a result of this messaging, mostly broadcast on television, significant Russophone populations in Crimea and the Donbass came to support either separatism from Ukraine or outright annexation by Russia. According to a 2014 study, viewing Russian television was strongly correlated with holding negative views of Euromaidan (Hale et al., 2014). A sizable proportion of the Russophone population in other regions of Ukraine, according to a National Science Foundation-sponsored study (O'Loughlin & Toal, 2016), believed pro-Kremlin narratives about the annexation of Crimea, the shooting-down of the Malaysian Airlines passenger plane, and the alleged domination of Ukraine's military and government by Nazis.

Russian Information Strategy in the 2020s

In preparation for the current war in Ukraine, Russia adapted its use of information warfare. In the weeks leading up to the full-scale invasion, Russian media operating in Ukraine—first Telegram channels and then traditional media—disseminated a narrative that Ukraine was preparing a major and violent attack on the separatist regions of Donetsk and Luhansk.

Russia relied on staged or fabricated videos and reports to legitimize this narrative. Explosions were consistently reported in the city centers of Donetsk and Luhansk, without any evidence being provided. Car bombs and other terrorist attacks within the breakaway republics were fabricated. A few days before the full-scale invasion, a video was posted on a pro-Kremlin Telegram channel of a supposed Ukrainian artillery attack on a civilian village. A villager could be seen screaming in pain, having lost a leg in the attack. In a few frames of the video, shown below, an attachment for a prosthetic leg can be seen, indicating that this crisis actor had in fact already lost his leg prior to the supposed shelling.



Source: Twitter User @OAlexanderDK

Russian television showed a helmet-camera video of an alleged firefight in which DNR soldiers halted an alleged Ukrainian offensive. It was later determined that the video was an edited version of a training exercise by the Russian military years earlier. Today, the dissemination of false images and videos is a key component of Russia's information warfare strategy.

Ukrainian Responses

Ukrainian responses to Russian information warfare were initially slow but have now taken on a dynamic and effective character that provides a model for other states subject to such influence. Responses include banning vectors of Russian information warfare, exposing misinformation, and conducting their own information campaigns.

Limiting and Banning Russian Mass Media: One of the most potent actions Ukraine has taken is limiting, sanctioning, and outright banning Russian-controlled mass media. Prior to the Euromaidan Revolution in 2014, Russian state-controlled media originating from Russia enjoyed widespread viewership in Ukraine. As many as 97% of Ukrainians received most of their news from television in 2014, according to survey data (Onuch, 2021, p. 3). Particularly among the Russian-speaking population, much of this television programming originated in Russia.

In 2014, the Ukrainian National Council for TV and Radio Broadcasting issued regulations banning several pro-Russian television channels that broadcasted disinformation. In February 2015, Ukraine's legislature passed a law banning Russian propaganda from Ukrainian television. That same year, the hardwired, analog cable connections between Russia and Ukraine that had allowed Russian media to access Ukraine were cut. By 2015, Ukraine had been almost entirely cut off from directly controlled Russian media originating from Russia.

However, pro-Kremlin indigenous Ukrainian mass media remained, the most potent of which were a series of television stations owned by Putin-friendly Ukrainian oligarch Viktor Medvedchuk. In February 2021, President Volodymyr Zelensky sanctioned three pro-Kremlin television stations owned by Medvedchuk and associated with the pro-Russian opposition party Za Zhizn (For Life): 112 Ukraine, NewsOne, and ZIK TV. Ukraine's sanctioning and banning of Russian-directed mass media, particularly television stations, has removed millions of Ukrainians from Russia's information warfare audience.

Exposing Misinformation: Civil society groups have also joined the fight against Russian information warfare in Ukraine by exposing misinformation and pushing to increase media literacy. The Media Reform Center at the Mohyla School of Journalism at the National University of Kyiv was established in 2014 and operates programs to increase media literacy and warn the public of the dangers of misinformation and propaganda. The center runs fact-checking workshops for journalists, public officials, and students in many cities across Ukraine.

StopFake.org, also founded in March 2014, is a website operated by Ukrainian academics, students, journalists, and media experts dedicated to exposing misinformation and debunking Russian narratives in Ukrainian media. Since its founding, the organization has debunked over 4,000 false stories, images, and videos originating from Russia or produced by Russian agents in Ukraine. One of its most prominent exposés was that of a video apparently of a Russophone mother in Ukraine grieving her child, who had supposedly been crucified by Ukrainian soldiers. StopFake was able to verify that the mother in the video was in fact a Russian television actress. Another prominent success was the debunking of the widely circulated Russian claim that ISIS had established training camps in Ukraine with the approval of the "fascist" government.

StopFake also broadcasts a weekly television show on about 30 channels in Ukraine exposing the most outrageous misinformation of the week. A recently debunked narrative was that the Ukrainian government intended to print Hitler's face on its currency. Russian agents have reportedly attempted to hire journalists working at StopFake, indicating the Kremlin's awareness of the organization's effectiveness.

Conducting Pro-Ukrainian Information Warfare: In addition to countering Kremlin information warfare, Ukraine is endeavoring to conduct its own information campaigns in hopes that pro-Ukrainian memes, stories, and narratives will overpower pro-Russian ones. This component of Ukraine's strategy has become particularly prevalent since Russia's military build-up at the end of 2021.

President Zelensky has emerged in the conflict as a master communicator. Filming multiple daily videos addressing the Ukrainian people directly in his now-iconic green military shirt and stubble has become a tool to build unity and legitimize the government. Zelensky himself has taken part in the debunking of Russian misinformation about his own whereabouts by posting videos of himself roaming the streets of Kyiv.

Official Ukrainian government social media accounts have also actively conducted their own information campaigns. Memes have become a new front in information warfare. Recent memes posted by the Ukrainian government's official Twitter account, @Ukraine, for example, feature references to an episode of Seinfeld, Ukrainian national poetry, and even a Spiderman movie from the early 2000s. The Twitter account of Ukraine's Ministry of Defense posts videos of Lavrov's recent speeches justifying the war juxtaposed with images of the destruction of civilian areas in Ukraine.

The production value of such Ukrainian government-produced content is relatively high. The Ukrainian government publishes dozens of such memes, images, and videos every day, many of which make their way to Ukrainian television. The strategy here seems to be to flood social media feeds with so much high-quality, shareable, pro-Ukrainian content that Kremlin narratives are drowned out.

Pro-Ukrainian Misinformation

As pro-Ukrainian content continues to be enthusiastically disseminated by social media users and media outlets around the world, the Ukrainian government must take care to avoid propagating false narratives. In the opening days of the war, stories, images, and videos of an alleged Ukrainian ace fighter pilot— nicknamed the "Ghost of Kyiv"—credited with shooting down countless Russian aircraft were spread online. Many of the claims surrounding this pilot lacked evidence, and images and videos of the supposed fighter ace were found to be false. One video allegedly showing the "Ghost of Kyiv" shooting down a Russian plane was found to be taken from a video game called Digital Combat Simulator.

The story of the 13 defenders of Snake Island is another example of a widely disseminated pro-Ukrainian narrative. A video was shared online in late February of a radio conversation between the defenders of the island and a Russian warship. A Ukrainian defender's provocative alleged last words in reply to the Russian ultimatum to surrender instantly became a rallying cry in Ukraine and around the world. The story became more powerful once President Zelensky declared that the soldiers had died fighting to the last man. Mere days later, it was discovered that the 13 soldiers of Snake Island had in fact been taken as prisoners of war by the Russian military. To maintain credibility and legitimate control of the narrative, Ukraine should act to counter all forms of misinformation, even stories that are seemingly supportive of its cause.

Conclusion

Ukraine, perhaps more than any other country, has been a prime target of Russian information warfare for the past decade. Initially relying on traditional mass media, mostly television, to propagate its narratives, Russia has been forced by Ukrainian responses to adapt its strategies. By banning pro-Russian mass media, launching initiatives for media literacy, exposing misinformation, and activating its own information campaigns, Ukraine has severely limited the avenues for Russian information warfare in the country and worked to inoculate its domestic audience against misinformation. While Russian information warfare was until the mid-2010s relatively effective in shaping attitudes in Ukraine, especially among the Russian-speaking population, today its reach is limited and impact is relatively weak.

About the Author

Nash Miller is a graduate student at the Elliott School of International Affairs at George Washington University studying European and Eurasian Studies with a focus on Russian security. He received his B.A. in International Affairs from Brigham Young University in 2020.

Bibliography:

- Hale, H. E., Colton, T., Onuch, O., Kravets, N. (2014). Ukrainian Crisis Election Panel Survey (UCEPS).
- O'Loughlin, John, and Gerard Toal. "RAPID: Attitudes and Beliefs in Russian-Supported 'De Facto' States and Eastern Ukraine in the Wake of the Crimean Annexation." National Science Foundation, July 31, 2016.
- Onuch, Olga, Emma Mateo, and Julian G. Waller. "Mobilization, Mass Perceptions, and (Dis)Information: 'New' and 'Old' Media Consumption Patterns and Protest." Social Media + Society (April 2021).
- Osipian, Alexandr. "Historical Myths, Enemy Images, and Regional Identity in the Donbass Insurgency." Journal of Soviet and Post-Soviet Politics and Society 1, no. 1 (2015): 109–40.

ANALYSIS

Russian Information Warfare: The Case of Poland

By Jessica Brzeski (George Washington University)

DOI: 10.3929/ethz-b-000541999

Abstract

Poland presents an interesting case study for Russian information warfare, as Russia's strategies and methods carry deeper meanings given the long history of antagonism between the two countries. Polish strategies to counter Russian information warfare have been much more effective than those of other countries that have fallen victim to this war tactic. In Poland, the Law and Justice Party has been tightening control over the domestic political space and adding new physical structures—such as cybersecurity hardware, surveillance mechanisms, and new federal agencies—that have contributed to its efforts to combat Russian information warfare. At the same time, however, these methods have undermined the rule of law within Poland.

One of the greatest emerging threats to Polish national security over the past decade has been the increasing use of Russian information warfare, which aims to create instability by widening political and social divides both domestically and internationally. Given the nation's long history with Russia, Poland represents a significant case study of Russian information warfare. Over the last several decades, Poland has transformed from a satellite state of the USSR into an independent state that has joined the most important institutions of the liberal international order: the EU and NATO. These accessions have further strained Poland's already difficult relationship with Russia. Such hard feelings leave space for Russian information warfare to manifest in strategic ways and through various venues. However, the governing party in Poland, Law and Justice, has sought to combat Russian information warfare even as it works to undermine the rule of law domestically. This case study seeks to tally the effective measures Poland has taken to combat Russian information warfare while calculating the domestic costs.

A Long-Standing Contested Relationship

As a former satellite state of the USSR, Poland suffered under Soviet occupation for decades, fueling negative popular sentiments toward Russia. Once the USSR fell, Poland regained real independence for the first time in almost two centuries. The main objective of the newly formed Polish government was to create a foreign policy that protected this independence. Integration into the international liberal order and further promotion of democracy became the two pillars of foreign policy in newly independent Poland (Kacewicz and Wenerski 2017, pg, 13). In order to further these two goals, the new government sought to join the European Union (EU) and the North Atlantic Treaty Organization (NATO). These two institutions shape the way Poland approaches Russian information warfare.

As a NATO member state, Poland must bring its domestic laws into line with the international organization, which has resulted in the strengthening of domestic security measures focused on information security (Kogut et al. 2021, p. 70). In addition, NATO relies on member states to contribute to combating information warfare. One example of this can be found in the creation of the Center of Excellence NATO Cooperative Cyber Defense (CCDCOE), which promotes the implementation of new policies within the cybersecurity realm (Colesniuc 2013, p. 127).

Although the relationship has been contested in recent years, Poland's accession to the EU has provided the country with critical resources to further develop the legal and physical structures needed to combat Russian propaganda. Like NATO, the EU seeks to integrate the security infrastructures and information systems of every member state into a cohesive whole. This approach allows for member states like Poland to further strengthen the structures that support information security with direct resource allocation (Kogut et al. 2021, p. 75). A specific example comes from the creation of the Network of Computer Security Incident Response Teams: each member state must house a response group that works with the broader network of groups to secure information systems in member states and within the EU as a whole (European Agency for Cybersecurity 2022).

Russia's Tools and Strategies

Russia claims that the West was the "first mover" when it comes to using information warfare to gain political and military advantage. The Russian leadership considers the expansion of NATO, a decade of color revolutions, and a deeply integrated EU to be threats (Śliwa and Antczak 2018, p. 23). In response, Russia has devised a number of approaches that focus on Poland. These include:

- Cybersecurity Threats: Poland has witnessed a steady increase in attacks on hardware, such as govern-

ment servers, since the invasion of Ukraine began (Reuters 2022).
- Cyber Hacking: Efforts to leak data and critical information, with a view to adversely affecting the nation, include a government-wide leak in June 2021 (AP News 2021).
- Media / Online Warfare: Campaigns seeking to create countering narratives to inflame divisions, such as an extensive anti-NATO campaign (The Guardian 2020).
- Historical Memory Warfare: Altering or erasing historical facts with false narratives (Sukhankin 2020).

These four tactics define Russian information warfare against Poland. Russian propagandists use different tactics for different audiences; in the case of Poland, the tactics used are a mix of those seen in Western countries such as the United States (i.e., media/online warfare) and those seen in neighboring countries such as Ukraine (i.e., historical memory warfare). Ultimately, the goal of Russian information warfare in Poland can be summarized as attempting to destabilize national security by impugning information security through various outlets that call into question historical, political, and social aspects of Polish statehood.

Impact of Russian Information Warfare in Poland

Russian information warfare has negatively affected Poland in various ways, ranging from intelligence leaks to the physical destruction of historical landmarks. Historically speaking, Poland has ties with Russia, but these are less significant than those Russia has with Ukraine, making the desired outcome of Russian information warfare different. Poland and Russia have frequently fought over various issues, and given the significant technological developments of the past two decades, this conflict has spilled into the field of information security. Polish identity has also changed significantly since the fall of the USSR, with the country's accession to the EU and NATO allowing for Russian information warfare to be dispersed within Poland in ways more similar to the countries that uphold these pillars of the liberal international order (Čižik 2017, pg.15). Thus, Poland has fallen victim to Russian information warfare in a blend of ways, as both a historical adversary and a now-Westernized nation. The most immediate impacts of Russian information warfare on Poland have been:

- Weakening Hardware Network: Poland's information technology and computer networks have been compromised due to their general accessibility and openness, making it possible for hackers to leak government information (Chojnacki 2012, p. 56–57).
- Creating Social Instability: Russia's use of media/online warfare and historical memory warfare further support certain narratives of the Law and Justice Party, which itself benefits from inflaming political divisions within Poland (Lucas and Pomeranzev 2016, p. 30).
- Intensifying Multilateral Tensions: The inflammatory domestic effect of Russian information warfare spills over into Poland's relationships with regional partners such as Ukraine (Belavusau et al. 2021, p. 19–20).

The above impacts have greatly tested the integrity of Poland's internet infrastructure and the population's ability to resist Russian information warfare. Ironically, Poland's ruling Law and Justice Party itself benefits from the anti-Western and anti-liberal narratives propagated by Russian information warfare.

Poland's Response

The Law and Justice Party has played a proactive role in countering Russian propaganda, which has had the effect of undermining the rule of law within the country. Primary counter-tactics to Russian information warfare by Poland include, but are not limited to:

- Tighter Legal Restrictions: The National Security Strategy of 2014, National Anti-Terrorist Programme (NATP) for 2015–2019, and the Strategy for the Development of the National Security System of the Republic of Poland (2022).
- Restricted Access: The Act on Anti-Terrorist Activities of 2016, the creation of the Anti-Terrorist Center, and the Government Center for Security have all increased government surveillance of Polish society.
- Media Curation: The Law and Justice Party has sought to impose media control, including attempting to take down the biggest independent television company in Poland (Discovery+) in 2021.

Conclusion

Overall, Polish measures to counter Russian information warfare have primarily been taken through the legal system and internet hardware. However, the Law and Justice Party has implemented certain legal restrictions that allow it to increase surveillance of the population and clamp down on critical media outlets. Therefore, in the case of Poland, combating Russian information warfare has come at the price of the rule of law.

About the Author

Jessica Brzeski is a graduate student at the Elliott School of International Affairs pursuing her M.A. in International Affairs with a focus on U.S. Foreign Policy and European/Eurasian Affairs. Previously, she earned a B.A. at Loyola

University Chicago in Global and International Studies and French Language, during which she studied abroad in Sydney, Australia, and Paris, France. She has held various positions within the sphere of international relations.

References

- Anon, 2020. Russia-aligned hackers running anti-Nato Fake News Campaign – Report. *The Guardian*. Available at: https://www.theguardian.com/technology/2020/jul/30/russia-aligned-hackers-running-anti-nato-fake-news-campaign-report-poland-lithuania (Accessed March 23, 2022).
- Anon, 2021. CSIRTS network. *ENISA*. Available at: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network (Accessed March 18, 2022).
- Anon, 2021. Polish intelligence agencies link cyberattack to Russia. *AP NEWS*. Available at: https://apnews.com/article/europe-russia-intelligence-agencies-technology-government-and-politics-261df587ec9f93e781be8203a083eea1 (Accessed March 23, 2022).
- Anon, 2022. Poland sees more cyberattacks on government servers, official says. *Reuters*. Available at: https://www.reuters.com/technology/poland-sees-more-cyberattacks-government-servers-official-says-2022-02-25/ (Accessed March 23, 2022).
- Belavusau, U., Gliszczynska-Grabias, A. and Mälksoo, M., 2021. Memory laws and memory wars in Poland, Russia and Ukraine. *Jahrbuch des öffentlichen Rechts, Forthcoming*. 1–22.
- Čižik, Tomáš, 2017. Russian information warfare in central Europe. *Information Warfare–New Security Challenge for Europe. Bratislava: Centre for European and North Atlantic Affairs*. 8–34.
- Chojnacki, Włodzimierz, 2012. Future cyberspace war and its impact on Polish Armed Forces. *Zeszyty Naukowe/ Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki*. 53–61.
- Gasztold, A. & Gasztold, P., 2020. The Polish Counterterrorism System and Hybrid Warfare Threats. *Terrorism and political violence*. 1–18.
- Kacewicz, Michał and Łukasz Wenerski, 2017. Russian soft power in Poland – The Kremlin and pro-Russian organizations. *Political Capital*. 1–58.
- Kogut, B. et al., 2021. Information Security in Poland and in the European Union: Administrative and Legal Conditions. *European Research Studies Journal XXIV*. (2). 68–77.
- Lucas, Edward, and Peter Pomeranzev, 2016. Winning the information war. *Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. Washington: The Center for European Policy Analysis*. 1–66.
- Sukhankin, Sergey, 2020. Russia's "Memory wars", Poland, and the forthcoming 75th Victory Day. *ICDS*. Available at: https://icds.ee/en/russias-memory-wars-poland-and-the-forthcoming-75th-victory-day/ (Accessed March 23, 2022).
- Śliwa, Zdzisław, and Anna Antczak, 2018. Military Domain as a Component of Information Warfare. *Kaitseväe Akadeemia*. 16–17.
- Świątkowska, Joanna, 2017. Cybersecurity Statecraft in Europe: A Case Study of Poland. *Georgetown journal of international affairs*. 18 (3), 83–94.

ANALYSIS

Putin's Information War Against the United States

By Jacqueline Evans (George Washington University)

DOI: 10.3929/ethz-b-000541999

Abstract:
Information warfare between the United States and Russia is not a new phenomenon. However, recent developments, including an increase in Russia's disinformation activities, the social media revolution, and the invasion of Ukraine have created challenges for the United States, forcing officials to reevaluate current policies and develop new innovative strategies to combat the Kremlin's information warfare attacks.

A Strengthening Anti-American Campaign

Since taking power, Vladimir Putin has increased Russian efforts to weaken democratic institutions and Russia's perceived enemies via such informational warfare tactics as disinformation, propaganda, false flag attacks, and cyber-attacks. These measures, coupled with the widespread use of social media, have impacted numerous democratic nations. Yet recent interference in elections, including in the United States in 2016, and Russian-backed misinformation have highlighted gaps within American defense policy. As such, this article will examine the history of information warfare between the US and Russia, the threat posed and tools employed against the US, as well as the challenges and necessity of creating an all-encompassing response.

History of Information Warfare Between the United States and Russia

During the Cold War, both the US and the Soviet Union used covert disinformation tactics to challenge each other's ideological systems and gain influence around the world. Both nations spread conspiracy theories and rumors, distributed propaganda literature, set up front groups, carried out political operations, and engaged in election interference (Ward, Pierson, Beyer, 2019, p. 4–5). These tactics were not intended solely to target the domestic audience in the opposing country, but rather aimed at weakening alliances and partnerships to create division and make foreign nations question their relationship with either the US or the Soviet Union.

Information warfare concerned American officials so much that a working group, the Active Measure Working Group (AMWG), was created to combat Soviet misinformation by gathering information, analyzing reports, and then publicizing the evidence of interference and Soviet-created disinformation materials to educate the government and the public (Ward, Pierson, Beyer, 2019, p. 7).

There are some similarities between information warfare during the Cold War and today. With the rise of social media, however, the measures that worked in the 20th century are not necessarily effective any longer. The internet and social media have made it much more difficult to address disinformation because individuals can deliberately or inadvertently share conspiracy theories, propaganda, and fake news with thousands of people while circumventing traditional gatekeepers. Additionally, due to the openness of American society and the separation between government and businesses, the responsibility to monitor and remove misinformation posts lies with Big Tech rather than the government. The new ability of people to communicate among themselves rather than through traditional mass media and the power of platforms like Facebook, Twitter, and TikTok make the current environment very different from what existed previously.

Russia's Information Warfare Threat

Even though Russian information warfare is not a new concept, it still poses a massive risk to U.S. democracy and its ability to act on the international stage. To better understand the threat, it is important to understand why Russia is using informational warfare against the US, what Russia's goals are, and what the Kremlin is targeting.

All actions taken by the Kremlin are carried out to achieve Russia's geopolitical goals, including preserving its zone of influence in the countries of the former Soviet Union, attaining desirable opportunities to extend Russian sway internationally, expanding the Russian economy, and protecting Russian culture and society from information interference and psychological attacks (Gurganus and Rumer, 2019). To achieve many of these goals, Putin believes that Russia must undermine the standing of the US domestically, in Europe, and around the world, as the Kremlin sees the US as pursuing policies to maintain American hegemony and isolate Russia (Wojnowski, 2021).

At its core, Russia seeks to use information to exert psychological influence over individuals, societal groups, nations, and multilateral institutions (Saradzhyan, 2021). Therefore, Russia's information warfare targets U.S.

democracy to create internal divisions, increase political polarization, influence elections, and discredit democratic institutions, as well as strain relations between the US and its allies/partners through misinformation campaigns within and outside the US that exacerbate tensions and undermine coalitions (Wojnowski, 2021).

Essentially, Russia's goal in the US is to create so much polarization and division that Americans come to doubt the legitimacy of democracy and their government. Internationally, Russia hopes to weaken Western coalitions by promoting information that makes allies and partners question each other.

Tools Employed by Russia

To increase its impact, the Russian information warfare toolbox contains country-specific elements. Thus, the tools used against Poland, say, are going to be slightly different than the tools used against the US. The three main tools used against the US include the weaponization of social media, the use of proxy media sources, and cyber-attacks.

The Weaponization of Social Media: Arguably the most-used and best-known tool is the weaponization of social media platforms, including Facebook, Instagram, Twitter, and TikTok. This is achieved by amplifying division regarding protest or civil society disputes, supporting and contributing to disinformation campaigns that undermine faith in institutions and official government reports/information, as well as inflating domestic debates (U.S. Department of State, 2020 p. 8–9). Russia hopes that spreading misinformation and conspiracy theories on social media platforms will stoke division and polarization amongst Americans.

This is a serious issue, as an estimated 72% of Americans use some form of social media daily with about 53% obtaining news from social media (Pew Research Center, 2021; Shearer, 2021). Usage of social media combined with social media algorithms promotes personalized and popular content, meaning that Russia's weaponization of information has a chance of reaching and influencing millions of Americans (Meserole, 2018). Complicating matters further, users can share content not only on the original platform, but also on other platforms, making it difficult for companies to stop the spread of misinformation. Moreover, a study on misinformation and Twitter found that inaccurate information spreads faster and reaches more users than accurate information (Vosoughi, Roy, and Aral, 2018, p. 1147).

It is important to note that the weaponization of social media impacts not only American elections and politics, but also such societal issues as COVID-19 information, conversations about race, and immigration. The number of contentious issues within the US has allowed Russian operatives to both spread misinformation and amplify contention by posting controversial opinions that further divide Americans.

Proxy Media Sources: Russian operatives also use proxy media sources to extend their reach and make misinformation seem more credible. This tool entails spreading information through Russian-backed media outlets and Western media outlets knowingly or unknowingly reproducing Russian narratives.

Numerous Russian-backed media outlets operate in English and reach American audiences. Some of these sources, such as RT and Sputnik, are known Russian-backed media sites, while others are sites that average individuals may not realize have a connection with the Kremlin (U.S. Department of State, 2020). Websites including Strategic Culture Foundation, Global Research, New Eastern Outlook, and News Front are all Russian propaganda sites that operate in such a way that average users may not recognize the Kremlin connection (Joscelyn, 2020).

Aside from Russian-backed media outlets, there are also media platforms that knowingly and unknowingly spread Russian propaganda. This can occur in a couple of ways. First, a media outlet or journalist can knowingly spread information that is not fact-checked and promotes a pro-Russian narrative. For example, disinformation regarding COVID and the recent invasion of Ukraine that originates from Russia has been included in American news podcasts and news shows, including shows on Fox News (Brandt, Danaditya, and Wirtschafter, 2022). Although these individuals may not know that the information is false when they first report it, there are instances where they have continued to spread the information even after it has been debunked, thereby aiding in the spread of Russian misinformation.

News outlets can also inadvertently spread misinformation by giving air coverage to certain stories that aid Russia in weakening the relationship between nations. For example, according to a Polish expert, Russia frequently tries to divide Poland and the West by promoting claims that Poland is a far-right country (Polish Professor, 2022). Although it is important to highlight when the Polish government or other governments restrict civil liberties, it is also important that news outlets investigate the source of material and ensure that it does not inadvertently promote Russian talking-points.

Cyber-Attacks: Russia is notorious for using cyber-attacks and cyber-led efforts to create division and chaos within the US. Tactics include hacking and releasing hacked materials to disseminate damaging or sensitive information in order to make Americans question their government, institutions, or individuals (State Department, 2020). An example of this is the hacking of the Democratic National Committee (DNC) in 2016: Russian operatives hacked the DNC's computer server and stole emails in the hope that it would damage presidential candidate Hillary Clinton's chances and thus help candidate Donald Trump (Director of National Intelligence, 2017). In the end, U.S. intelligence was able to determine that the cyber-attack had been carried out by Russia with a view to interfering in the election.

Together, these three tools have enabled Russia to successfully create and increase divisions between Americans. Additionally, the use of these tools makes it difficult for the US to attribute each effort to the Kremlin and Vladimir Putin, giving them some form of deniability.

The American Response

The increase in informational warfare efforts has not gone unnoticed by the US. Intelligence officials and members of the federal government recognize the risk these efforts pose to U.S. security. As such, these officials have scrambled to respond to the threat to protect democracy and the American way of life.

In 2016, under Executive Order 13721, President Obama created the Global Engagement Center (GEC) (Department of State Archive, 2001–2017). The GEC is housed in the State Department and was originally tasked with combating misinformation and messaging from ISIS (Department of State Archive, 2001–2017). However, the reach of the GEC expanded following the election interference conducted by Russia in 2016. Today, the GEC publishes reports outlining Russian information warfare tactics around the globe (U.S. Department of State, 2020). Most recently, as part of the effort to combat Kremlin misinformation regarding the invasion of Ukraine, the GEC and other offices of the State Department have started releasing Kremlin Disinformation Bulletins to document Russia's disinformation campaign in real time (United States Department of State, 2021).

Additionally, in 2018, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) created an inter-agency task force to counter Russian misinformation (Bodine-Baron, Helmus, Radin, and Treyger, 2018). This task force brought together DHS's Countering Foreign Influence Task Force and DOJ's Cyber Digital Task Force.

The intelligence community has also employed the tactic of revealing intelligence information regarding Russian information warfare campaigns as they occur to alert and warn both the public and private sectors. This occurred during the run-up to the 2020 election, when officials at the FBI and CIA warned that Russia was once again going to try and further polarize Americans and interfere in the election (National Intelligence Community, 2021). Additionally, the intelligence community and the Biden administration have in real time warned of misinformation efforts regarding COVID-19 and the invasion of Ukraine. Although such efforts are still relatively new, many pundits and experts believe they could be useful in beating Russia at its own game and helping to stop the spread of misinformation (Ott, 2021).

Outside the intelligence community and executive branch, Congress has begun to address this issue by holding hearings regarding the threat, considering legislation, and pressuring social media companies and executives to do more to stop their platforms from being used as Russian tools. Proposed legislation has ranged from sanctions against Russia to efforts to make political ads and social media data more transparent (Bodine-Baron, Helmus, Radin, and Treyger 2018). However, due to polarization within Congress, many legislative efforts have stalled.

Finally, under pressure from the government and the public at large, private companies have stepped up their efforts to combat Russian disinformation, including by increasing content monitoring, flagging false information, adjusting what political ads can be posted and by whom, and labeling political ads so users know that they are ads and may contain misleading information (Bodine-Baron, Helmus, Radin, and Treyger, 2018).

Most of these tactics have been implemented in the last 4–6 years, meaning the US is still severely behind in addressing the scope of Russian information warfare. In addition to the delayed response to threats, there are also challenges posed by the democratic essence of the U.S. political system.

Challenges and Gaps in the American Response

The biggest challenge facing the US is the need to respond while protecting the civil liberties and freedoms enshrined in the Constitution. First, under the U.S. Constitution, citizens have the right to free speech. Although there are some restrictions, overall, there are protected rights on social media to say how you feel and like or repost what you agree with. Free speech and freedom of expression are important facets of liberal democracies; efforts by the federal government to limit what people can say, like, or post on social media will be seen by many as censorship. This makes it difficult for the government to stop individuals and official media accounts from advertently and inadvertently spreading Russian misinformation.

Moreover, past intelligence community scandals that exposed spying and monitoring of American citizens and journalists have made the public wary of allowing the intelligence community to monitor and engage in fact-checking activities on social media and traditional media. Notably, a lot of the recent distrust of the government regarding its ability to fairly and accurately monitor content has been exacerbated by successful Russian information campaigns that have sought to polarize Americans.

Lastly, as evidenced by the debates regarding universal health care, business regulations, and pressure on social media companies, a key pillar of the American system is the separation between the government and the private sector. This principle carries over to the ability to address Russian information warfare because unlike other nations or even the EU, where there are more options for the government to regulate the private sector, in the US this is frequently debated and sometimes frowned upon. Together, this means that although the government can pressure social media and news outlets to be more proactive in addressing Russian propaganda and misinformation, there are limits to how much the U.S. government can force the private sector to act (Bodine-Baron, Helmus, Radin, and Treyger, 2018).

Although the lack of a coherent and strong response to Russian disinformation can be attributed to the need to respond effectively while protecting civil liberty, the harsh reality is that up until 2016, the US was not paying sufficient attention to the information warfare that Russia was conducting.

Conclusion

The threat of Russian information warfare and gaps in American policy responses highlight the dire need for a more sound and cohesive response. Without this, Russia will continue to use information warfare to sow chaos by dividing Americans and weakening democracy. Although these efforts are not new, they have been facilitated by the social media revolution, which has made information-planting and -sharing as easy as a click of a button, with the ability to reach millions of people in minutes.

Putin will not stop his assault on foreign democracy merely because he has been caught. Rather, he will continue to adapt and find new ways of disseminating misinformation. There are lessons to be learned and tools the US can adopt from other countries that have been dealing with this threat for over a decade. Yet it will take efforts by the federal government, the private sector, media outlets, and ordinary citizens alike to effectively and efficiently counter Russian information warfare.

About the Author

Jacqueline Evans is an M.A. candidate at George Washington University studying International Affairs with a focus on U.S. Foreign Policy and European/Eurasian Studies. She also holds a graduate certificate in International Security from the University of Arizona.

Bibliography:

- Brandt, J. Danaditya, A. and Wirtschafter, V. (2022). *Popular podcasters spread Russian disinformation about Ukraine biolabs*. Brookings. Available at: https://www.brookings.edu/techstream/popular-podcasters-spread-russian-disinformation-about-ukraine-biolabs/
- Bodine-Baron, E., Helmus, T., Radin, A. and Treyger, E. (2018). *Countering Russian Social Media Influence*. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf
- Department of State Archive. (2001–2017). *Global Engagement Center*. Available at: https://2009-2017.state.gov/r/gec/index.htm.
- Director of National Intelligence. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. DNI. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf
- Gurganus, J. and Rumer, E. (2019). *Russia's Global Ambitions in Perspective*. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/02/20/russia-s-global-ambitions-in-perspective-pub-78067.
- Joscelyn, T. (2020). *How Effective is Russia's Disinformation?* Foundation for Defense of Democracy. Available at: https://www.fdd.org/analysis/2020/08/12/how-effective-is-russias-disinformation/
- Meserole, C. (2018). *How misinformation spreads on social media—And what to do about it*. Brookings. Available at: https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it/
- National Intelligence Community. (2021). *Foreign Threats to the 2020 US Federal Elections*. National Intelligence Council. Available from https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf
- Ott, Haley (2021). *Information warfare expert says the U.S. is finally countering Russia at its own game*. CBSNews. Available at: https://www.cbsnews.com/news/ukraine-russia-information-warfare-disinformation-stopfake/
- Pew Research Center (2021). *Demographics of Social Media Users and Adoption in the United States*. Pew Research Center: Internet, Science & Tech. Available at: https://www.pewresearch.org/internet/fact-sheet/social-media/?menuItem=c14683cb-c4f4-41d0-a635-52c4eeae0245.

ANALYSIS

Russian Information Warfare in the European Union

By Jesse Clarke, George Washington University

DOI: 10.3929/ethz-b-000541999

Abstract:

The European Union is one of Russia's prime subjects in the modern information war. Russia targets the EU using both covert and overt disinformation methods, while thematically focusing on divisive topics like member state sovereignty and the COVID-19 pandemic. Compared to other international actors, the EU's policy response has been relatively robust, focusing on increasing its populace's media literacy and working with tech companies to regulate disinformation on their platforms. Although ahead of many others, coordination and implementation issues inherent to the EU's structure have limited its ability to counter Russian disinformation in certain areas. This article aims to use the EU as a case study to contribute to the literature around viable policy options for combating Russian information warfare operations.

Long in the Crosshairs

The European Union (EU) has long been a target of Russian information warfare. From the time of Peter the Great, through Joseph Stalin, and now Vladimir Putin, Russia and its leaders have sought to influence how Europeans view their neighbors to the east. In a modern context, Russia's resurgence in the last decade as an actor hostile to the West has coincided with a dramatic uptick in disinformation operations in Europe meant to justify Russia's actions and provide viewpoints sympathetic to them. Representing over 60% of Europe's population and counting three former Soviet Republics and six former Warsaw Pact states among its members, the EU is uniquely situated to be a target of Russian information warfare. Thematically, much of Russia's information operations in Europe follow trends from elsewhere in regard to the overall desire to sow discord and division, although there are a few key differences. Additionally, the EU's close proximity to Russia and its supranational nature make it an important case study for global actors seeking to counter Russian disinformation. By analyzing the unique aspects of Russian information warfare in the EU, followed by the successes and failures of the EU's responses, some potentially viable policy options to counter Kremlin-based information operations can be illuminated.

How the EU is Being Targeted

As in many other locations, Russian information warfare toward the EU is both covert (i.e., the source is not known) and overt (the source is known). It is important to draw a distinction between these two methods, as they can vary drastically in both their approaches and their subject matter. Overt Russian disinformation in the EU mainly comes in the form of state-sanctioned propaganda originating from the Kremlin. It emanates largely from two predominantly English-speaking, state-owned media outlets—RT and Sputnik News—that Russia uses to spread narratives favorable to its government and contribute to the overall information battle. RT and Sputnik use both cable and satellite to propagate their messages, but their audience in the EU and abroad is mainly reached through social media (Golovchenko, 2020). However, following Russia's invasion of Ukraine in February 2022, the EU issued a blanket ban in early March on RT and Sputnik and stated that any outlets that continue to publish their content will be subject to fines. A few days earlier, tech giants like Facebook and YouTube had begun to restrict access to these channels on their platforms in Europe in retaliation for the invasion. Following these measures, it is unclear what impact Russian overt disinformation will have on the EU in the future; it is likely that the Kremlin will focus on covert methods going forward.

Russia's use of covert disinformation campaigns in the EU is much more difficult to track due to its secretive nature and the associated attribution challenges. The primary method focused on in the scholarly literature is Russia's use of fake accounts on Western social media, specifically Twitter (Golovchenko, 2020). These can take the form of "automated accounts, fake profiles, bots or 'army of trolls'" and have "the advantages of low cost, rapid spread and high impact" (Durach, 2020, p. 6). In the early 2010s, much of this covert information warfare took the form of purely fabricated stories, or "fake news," designed to either sow discord or promote a particular pro-Russian narrative. After many European governments adopted policies to combat fake news and invested in media literacy programs, however, social media companies started to regulate false content more stringently (Durach, 2020; Sarwein, 2020). This trend has caused some scholars to speculate that covert disinformation campaigns in the EU are moving toward selective amplification of real, often polarizing, news stories in place of the traditional fake news model (Sarwein, 2020).

The Themes of Disinformation

Thematically, Russian information warfare can vary greatly depending on its intended recipient, but many scholars have noted the foundational similarity of an attempt to "sow confusion, doubt, and to blur the boundaries between enemy and non-enemy, war and peace, in order to make the population question who is the enemy and whether they are at war" (Golovchenko, 2020, p. 4). Nevertheless, in the case of the EU, there are a few unique characteristics of Russian disinformation that are worth noting.

One common thread is efforts to push for self-determination and sovereignty among citizens of EU countries and, correspondingly, against EU centralization, in a narrative that depicts Brussels as a group of distant bureaucrats (Magdin, 2020). This takes the form of promoting nativist and nationalist sentiments, notably in European countries with deep pre-existing divisions (Spain, Belgium) or with historically shifting borders (Western Ukraine–Poland, Finland–Sweden, Transylvania–Hungary). In former Eastern Bloc countries like Romania and Poland, disinformation can also hark back to the communist era by playing on nostalgia and, in the case of Romania, highlighting the economic struggles brought about by adopting the EU's monetary model (Magdin, 2020). These narratives contribute to the anti-Western views that Russia seeks to embolden, while also attempting to rehabilitate Russian soft power in Eastern Europe by arguing that life was better for the average citizen under the Russia-led Soviet Union. Paradoxically, there has recently been an increase in Russian disinformation campaigns in support of discussions around EU "strategic autonomy," or the idea that the EU should take steps to create its own military capabilities in order to be less reliant on NATO. This is largely seen by scholars as a geopolitical attempt to undermine U.S. and NATO influence in Europe (Magdin, 2020). Anti-Western narratives are also seen in Russian information warfare surrounding the COVID-19 pandemic and vaccinations. Russia sought to improve its image by "comparing [its] handling of the pandemic to how Western governments have been handling it, in some cases by falsely representing the actions of the EU and its member states" (Pamment, 2020, p. 11). The efficacy of Western vaccines was also repeatedly questioned by disinformation campaigns in order to make Russia's Sputnik-V vaccine seem more effective by comparison.

How the EU is Responding

Compared to other actors impacted by Russian information warfare, the EU's response has been relatively strong. However, there are still a few key structural factors that limit the EU's overall success in combating disinformation campaigns.

Substantive EU policy on information warfare was first adopted as a reaction to the Russian annexation of Crimea in 2014 (Pamment, 2020). The annexation came in tandem with a barrage of disinformation campaigns on social media to garner support for the Kremlin's actions, and the EU perceived the Russian threat to be one worth addressing seriously. The EU's European External Action Service (EEAS) was the natural home for a new policy to address information warfare, as its Strategic Communications arm already housed two divisions related to the subject: the Communications Policy and Public Diplomacy division, which mainly "manages communications campaigns, internal communication, social media accounts, and digital platforms as well as public and cultural diplomacy," (Pamment, 2020), and the Task Forces and Information Analysis division, which provides analytical support for communications policies and focuses largely on southern and eastern Europe. At the time, neither of these divisions were adequately equipped to handle the threat of Russian information warfare. Thus, the East StratCom Task Force was created by the European Commission in 2015 specifically to "identify and expose Russia's disinformation campaigns" (Durach, 2020, p. 9). StratCom produces a weekly report flagging pro-Kremlin disinformation on its EUvsDisinfo website, and at the time of writing had an open-source database of over 13,000 examples of Russian disinformation ("EUvsDisinfo", 2022).

Given that many disinformation campaigns take place on social media websites, the EU has found it necessary to collaborate with private industry on some of its policies to counter Russian information warfare. When it comes to private companies and information warfare, some argue that it is best for corporations to self-regulate, while others claim that corporations cannot be trusted and that content on their platforms should be directly regulated by the state. The EU has opted for something in between, aptly titled "co-regulation" (Durach, 2020). The goal of this strategy is to bridge the public-private gap by finding "a compromise which allows the implementation of a series of measures by the internet platform companies, monitored by an authority" (Durach, 2020, pp. 9–10). In this vein, the EU created in October 2018 its Code of Practice on Disinformation, which is meant to serve as a guide of sorts for private companies regarding how they should regulate their platforms. Companies signed on to monitor five areas related to disinformation: online advertisements, political advertising, integrity of services, transparency for consumers, and transparency for researchers ("EU Code of Practice", 2018), however this policy has been criticized because companies self-report their progress rather than it being externally reviewed, leading to questions of efficacy. This highlights the importance of addressing the challenges brought about by the private sector's necessary role in adopting policy to counter disinformation.

A few months after the Code of Practice was introduced, the EU announced its Action Plan Against Disinformation in December 2018. This plan was structured around four key pillars: "improving the capabilities of Union institutions to detect, analyse and expose disinformation, strengthening coordinated and joint responses to disinformation, mobilising private sector to tackle disinformation, raising awareness and improving societal resilience" ("Action Plan Against Disinformation", 2018). The action plan also highlighted the need for East StratCom's mandate to be expanded and its funding increased, as well as calling for initiatives in the realms of media literacy and journalism (Pamment, 2020). Notably, the creation of a Rapid Alert System to detect disinformation threats and improve information-sharing was also proposed. This idea came to fruition in March 2019; the resulting system was "intended to connect to existing real-time monitoring capabilities inside and outside of the EU, such as the Emergency Response Coordination Centre and the EEAS Situation Room, as well as the G7 Rapid Response Mechanism and the North Atlantic Treaty Organization (NATO)" (Pamment, 2020, p. 9). While a useful tool in theory, the Rapid Alert System has unfortunately not lived up to its potential thus far. This is a result of the EU's largely decentralized nature, as it is up to individual member states to decide when and how to share information through the Rapid Alert System, and definitions of—and importance given to—Russian disinformation can vary wildly depending on the politics of the country. While effective for small coalitions of member states passionate about opposing disinformation, it has struggled to break through on a pan-EU level due to low engagement. This is indicative of a problem that plagues the EU across many of its policy areas related to information warfare, namely coordination and implementation (Saurwein, 2020). However, this may well change in the future, as the Russian invasion of Ukraine has united Europe against Russia in a way not seen in decades.

Conclusion

Overall, EU policy to combat Russian information warfare has been much more substantial and targeted than that of many other actors. The EU has benefited from a relatively early response to disinformation campaigns and has had time to refine its program. Its successes in this field have largely been based on clarity of mission, as well as transparency with its populace. Unlike other actors, the EU has not sought to mount counter-offensives in the realm of information warfare, but instead seeks to promote awareness of Russian efforts through media literacy programs and EEAS plans of action. Additionally, the EU has attempted to work alongside private companies through its co-regulation model to tackle disinformation.

However, the EU has necessarily been limited by problems of implementation and coordination. While it is easy for the EU to announce a useful policy like the Rapid Alert System, it is much harder to put it into practice due to the differing opinions of individual member states and the EU's inability to force them to comply. In any case, its model of decisive action centered around public awareness offers a helpful policy option for other actors seeking to combat Russian information warfare, while the clear gaps in its policy could be addressed if adopted by an actor with a stronger federal mandate.

About the Author

Jesse Clarke is a graduate student at International Affairs at George Washington University, concentrating on international security studies in Europe. He received his Bachelor of Arts in Political Science and International Studies from the University of Oregon in 2020.

Bibliography

- "EU Code of Practice on Disinformation," European Commission, September 26, 2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.
- "EUvsDisinfo," European Union East StratCom Task Force, https://euvsdisinfo.eu.
- Fabrizio Di Mascio et al. (2021) Covid-19 and the Information Crisis of Liberal Democracies: Insights from Anti-Disinformation Action in Italy and EU. *Partecipazione e conflitto*. 14 (1), 221–240.
- Flavia Durach et al. (2020) Tackling Disinformation: EU Regulation of the Digital Space. *Romanian journal of European affairs*. 20 (1), 5–20.
- Golovchenko, Y. (2020) Measuring the scope of pro-Kremlin disinformation on Twitter. *Humanities & social sciences communications*. 7 (1), 1–11.
- High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan Against Disinformation," 1.

- Pamment, J., 2020. *The EU's role in fighting disinformation: taking back the initiative* (Vol. 15). Carnegie Endowment for International Peace.
- Radu Magdin (2020) Disinformation campaigns in the European Union: Lessons learned from the 2019 European Elections and 2020 Covid-19 infodemic in Romania. *Romanian journal of European affairs*. 20 (2), 49–61.
- Saurwein, F. & Spencer-Smith, C. (2020) Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe. *Digital journalism*. 8 (6), 820–841.
- Wagnsson, C. & Hellman, M. (2018) Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare: Normative Power Europe Caving In? *Journal of common market studies*. 56 (5), 1161–1177.

ANALYSIS

Russian Information Warfare: Policy Recommendations

By Jesse Clarke, Jacqueline Evans, Jessica Brzeski, and Nash Miller (all George Washington University)

DOI: 10.3929/ethz-b-000541999

Abstract

This final article on Russian information warfare presents policy recommendations that can be adopted to combat and respond to information warfare. Each case study exhibits unique circumstances that illuminate potential policy options for counteracting Russian disinformation campaigns. After analyzing both the successes and failures in each case study, the following policy recommendations emerged: transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation. These policy recommendations provide a broad framework for all countries facing a similar threat.

Introduction

Russian information warfare is an existential threat to liberal democracies that value peace, stability, and the rule of law. Due to the widespread, global nature of Russia’s information operations, countries worldwide have been impacted by these campaigns. Depending on the target, distinct circumstances can dramatically alter the way that Russian disinformation manifests itself. However, in analyzing four case studies of actors that have been especially impacted by information warfare—namely Ukraine, Poland, the United States, and the European Union—recurring themes of what has (and has not) been successful in countering the Kremlin emerged. Among the most notable are: transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation. Due to their success in widely varied contexts, these policy options can hopefully serve as tools for any potential actor looking to counter Russian information warfare now and in the future.

Transparency

The first policy that all governments, institutions, and agencies should adopt is transparency. One of Russia’s goals is to weaken society by creating division and doubt about what is true and what is false. This is particularly evident when you examine how Russia has used information warfare to make average citizens question the legitimacy of their own governments and the information that they receive from them. Although a vital part of democracy is the freedom to question the information of a government, Russia has exploited this to foment division and make people doubt the very legitimacy of their own governments and whether they truly support the rule of law.

The best way to combat these efforts is by being transparent with the public, providing factual evidence that backs up an official government claim. The United States has attempted this strategy through its intelligence community’s bid to shine a light on Russian disinformation campaigns in advance of the February 2022 invasion of Ukraine, sometimes before the events had even happened. Although met with uncertainty at first, when many of these events eventually transpired, this strategy proved itself an effective tool for transparency.

The European Union also seeks to be transparent with its populace by tracking and exposing examples of Russian disinformation on its website EUvsDisinfo, which currently has a database of over 13,000 cases. The EU emphasizes the explanatory rather than inflammatory nature of EuvsDisinfo, which is run by the body's East StratCom Task Force. The EU values transparency and public awareness of disinformation above all else, and the organization publicly states on its website that no counter-information operations are conducted.

Information warfare is inherently based on lies, deception, and misdirection. For this reason, policy intended to counter it should focus on being as transparent as possible with the public in order to cut through the fog and build trust among citizens.

Preemptive Information-Sharing

Another policy option that has thus far shown promising results in combating Russian information warfare is the use of preemptive information-sharing. This policy option calls upon members of the government and intelligence community to preemptively release information to the public once the intelligence agencies are warned of a particular misinformation or disinformation campaign that Russia is planning to implement. Preemptively warning about an upcoming Russian information operation alerts both the general public and foreign countries ahead of time, thus enabling them to prepare for and weaken Russia's operation.

Currently, this strategy is successfully being implemented by the US in regard to Russia's invasion and the Kremlin's response to the global sanctions. Two key examples that demonstrate its overall success include the US releasing intelligence that Russia was planning to use a false flag operation to justify the invasion and President Biden's warning to American corporations that Russia was going to disrupt the US via a hacking campaign. In both cases, the policy of preemptive information-sharing informed the relevant parties and the public of the Kremlin's antics, thus reducing the attack's likelihood of success and giving actors time to steel themselves against it.

Other countries and multilateral organizations should employ this policy, as it essentially beats Russia at its own game. By releasing reports that Russia intends to carry out a misinformation or disinformation attack, it makes the public aware of the threat, thereby making information warfare less effective because individuals in society are less likely to fall victim to the false narrative and propaganda slogans.

Media Literacy Education

Campaigns to promote media literacy can be a potent force in inoculating audiences against information warfare. If given the proper intellectual tools, audiences can be taught to identify misinformation, independently fact-check, and compile trustworthy verified sources.

Latvia, which has been on the front line of Russian information warfare for years, has successfully used media literacy education at schools and universities. Similarly, since the annexation of Crimea and invasion of the Donbass in 2014, Ukrainian civil society groups have successfully implemented a number of programs aimed at improving media literacy.

Universities, schools, and other organizations can conduct short courses or workshops for students, journalists, and political activists to effectively recognize misinformation. Civil society groups and journalist organizations have also found success in exposing and disproving Russian misinformation using verifiable facts. Openly exposing misinformation narratives can drown out and delegitimize information warfare campaigns, and can be an effective alternative to censorship, which raises civil liberties concerns.

As governments scramble to protect their populations from information warfare, media literacy education campaigns—starting from an early age and conducted by balanced and trusted organizations—can have a major impact.

Private-Sector Engagement

Engagement with the private sector has shown itself to be a crucial aspect of countering Russian information warfare. Since many covert disinformation campaigns are conducted via social media, the corporations that run these websites and apps necessarily have a role to play in coordinating responses to this threat. There are many schools of thought on how the public and private sector should interact within this space, with some arguing that the public sector should simply dictate policy to corporations and others advocating for allowing companies to self-regulate their content.

The European Union has opted for something in between, called co-regulation, and this model serves as a useful example for how states may approach policy to counter information warfare in a pragmatic way. The co-regulation model seeks to find areas of potential cooperation with social media companies in a way that aims to foster goodwill and keep them on the side of governments in the fight against disinformation. The EU has attempted to implement this through its Code of Practice, which serves as a guide for how private companies should regulate disinformation in key areas such as political advertising and general integrity of services.

The Code of Practice is far from perfect: critics have noted that the progress companies make in tracking disinformation areas is largely self-reported and is not subject to strict enforcement. However, it provides a helpful framework for how states and international actors can orient policy against disinformation in a way that includes the private sector. Large social media companies must be considered in any attempt to counter Russian information warfare due to how heavily the

Kremlin relies on these media to conduct its information operations. Many of these companies have a vested interest in regulating disinformation, but their concerns are primarily financial and are not inherently opposed to the idea of Russian-originated accounts stoking divisive topics on their platforms. Policies that bring the private sector into the fold as a collaborator against disinformation, like the EU's Code of Practice, are preferable to allowing corporations to be the sole arbiters of what should and should not be allowed on their platforms.

Multilateral Cooperation

The scope of information warfare has evolved beyond the borders of one country, with impacts spreading globally. Therefore, for a country to effectively combat information warfare of any type, a multilateral effort must be considered. This entails countries coming together in creating effective solutions to combat information warfare by implementing standards and structures through shared experiences. Not only does multilateral cooperation to combat information warfare strengthen efforts, but it also holds countries accountable in their own domestic processes. Overall, countries should make multilateral cooperation one of their key solutions to combating information warfare

In the case of Poland, binding obligations to multilateral security measures within the EU and NATO have strengthened domestic information security structures. These include physical and legal implementations that help combat impending threats and destruction caused by Russian information warfare. A desire to measure up to the legal standards of the EU and NATO has not only impelled the initiatives taken by Poland in the security realm, but also inspired domestic enterprise. In addition, as a member state of both organizations, Poland has also contributed to their information security. Therefore, a multilateral approach to Russian information warfare fosters greater accountability and ingenuity in combating the various associated threats.

Multilateral cooperation in the face of information warfare will resolve a variety of issues when it comes to combating this evolving threat. As globalization has spread, so too have the platforms and techniques of information warfare evolved to impact a series of actors ranging from online citizens to government institutions. The case study of Poland perfectly exemplifies why multilateral cooperation would benefit countries as they attempt to counteract the various derivative threats of information warfare. An approach that seeks multilateral cooperation would strengthen the legal and physical structures of countries while implementing domestic accountability. Of course, multilateral cooperation is not a perfect solution, but it offers a pre-established platform that would provide the basis for further problem solving.

Conclusion

As demonstrated in this series of articles, Russian information warfare poses a massive threat to the future of democracy. The danger lies in the Kremlin's ability to use various methods and tools that target each nation differently, thus making a global response more difficult. That said, as laid out in the previous sections, the successes and failures of democracies around the world show which countermeasures work and, therefore, what policies should be adopted to limit Putin's ability to further divide the democratic world. By adopting transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation, countries can combat information warfare while protecting vital civil liberties. Information warfare is here to stay and will continue to evolve as social media and the internet continue to change. Thus, states must develop strong responses now and prepare for future threats.

About the Authors

The authors are all pursuing MA degrees in international affairs at the George Washington University's Elliott School of International Affairs.

Acknowledgement

We would like to thank Robert Orttung of the George Washington University for all of his support and advice throughout this project. Additionally, we would like to thank the George Washington University for providing funding for our group to travel to Warsaw and Krakow in order to interview experts in Poland about the Polish and Ukrainian responses. Finally, to all of the people we have interviewed, thank you so much for your time and fascinating insights.

ANALYSIS

Shaping Online News Recommendations in Russia: The Yandex.News Controversies[1]

By Françoise Daucé (School for Advanced Studies in the Social Sciences (EHESS)) and Benjamin Loveluck (i3-SES)

DOI: 10.3929/ethz-b-000541999

Abstract

In Russia, numerous controversies have arisen since 2012 around the political role of the aggregator Yandex.news in prioritizing media news. Through its algorithm, this service is suspected of contributing to the decline of information pluralism for political purposes. These suspicions have only grown with the start of the war in Ukraine.

Where Google Does Not Dominate

Russia is among the few countries in the world where Google does not dominate the online search industry. In 2020, the Russian-language equivalent, Yandex, held just under half the market share (about 45 percent).

Yandex has long benefitted from a certain degree of autonomy, and its founders have even, at different moments, expressed political disagreement with the Kremlin. However, as a national economic champion and a key player in the organization of information, it has found itself under tight scrutiny. This has been particularly true since the 2011–2012 protests against electoral fraud and the 2014 annexation of Crimea, which also represented turning points for Russia due to the increased control exerted over the media, Internet, and civil society (Oates, 2013; Soldatov and Borogan, 2015; Wijermars and Lehtisaari, 2020).

A case in point is the Yandex.Novosti ("Yandex.News") aggregator—the Russian equivalent of Google News, launched in 2004—which is the focus of this article. When they first appeared, search engines and recommendation systems such as aggregators were designed as tools that would make the diversity of content on the Web more manageable. As a vast body of research has shown, however, these platforms occupy a strategic place and have become key intermediaries in channeling information to end users *qua* citizens. Thus, they wield a form of power in shaping users' perception of social reality that scholars, policymakers and civil society alike are still in the process of defining. With the start of Russia's war against Ukraine on February 24, 2022, the role of Yandex.News in controlling the media agenda in Russia has become an even more crucial issue.

Algorithmic Gatekeeping in Digital Media Ecosystems

The Yandex.News aggregator can be described as an *automated news recommender system*. The best-known example of such a service is the Google News aggregator, which was first launched in 2002 and taken out of beta in 2006 (Bharat, 2006). Initially, the service aimed to provide a broad overview of trending news by presenting users with "clusters" of related articles. As of 2021, the service indexed tens of thousands of news websites around the world and was woven into Google's main web search service.

Google and Yandex alike have generally presented their services as "neutral," but such claims to objectivity have been criticized for various reasons. For the past decade, because of their increasingly powerful personalization features, some of the main Web services—and particularly Google's search engines—have been suspected of entrapping users in "filter bubbles" and "echo chambers" (Pariser, 2011; Bozdag, 2013). By making users oblivious to certain types of information or to alternative perspectives, and by sometimes reinforcing existing prejudices or biases, these services arguably undermine the public sphere. Search algorithms and automated recommender systems have also been criticized for promoting outrage and conspiracy theories, with the YouTube recommendation algorithm, for instance, being presented as "the great radicalizer" (Tufekci, 2018).

However, the reality of these phenomena is difficult to assess precisely (Flaxman et al., 2016; Bruns, 2019), particularly in the case of search engines, which have also been shown to increase information diversity (see Fletcher and Nielsen, 2018). The algorithms deployed by these platforms can therefore be perceived as an "invisible hand," deciding which topics will be singled out as relevant and which news outlets will be pushed to the forefront according to sometimes unfathomable criteria—profoundly affecting the nature of journalism in the process, as professionals adjust the form and nature of their published content in line with these constraints

[1] A longer version of this article has been published online: Daucé, Françoise, and Benjamin Loveluck. "Codes of conduct for algorithmic news recommendation: the Yandex. News controversy in Russia." First Monday (2021).

(Brake, 2017; Christin, 2020). In the Russian political context, the issue raised by the Yandex.News aggregator is acute: could it be manipulated for political reasons, either through direct interference with the results or by fooling its algorithm?

Yandex.News as Political Controversy

Russia's political leadership has targeted Yandex.News through various policies and legal initiatives since 2014. Yandex.News presents a selection of topics and articles that purport to reflect the themes most widely covered by the media at any given moment. To do so, it processes the information published by a range of (mainly Russian) online media. Yandex.News was launched in 2004 and was initially a pilot project led by a team of computer scientists and linguists who had been hired to develop named-entity recognition and extraction in the news. The Yandex.News team claims that the algorithm works in the absence of human intervention. News from partners is gathered into topics through the algorithm's clustering process, which analyzes keywords and facts using three main criteria: citation rate, recency, and informativity. A Top 5 of its aggregation results is always visible on the Russian version of the Yandex homepage, just above the search box. In 2017, according to Grigori Bakunov, Yandex Technical Director, "The daily audience of the five news items that appear on the Yandex homepage is the same as the homepage—approximately 20 million people, depending on the day. Six million visit the Yandex.News page daily."

However, the controversies that arose after 2012 put an end to public belief in the objectivity of the aggregator. That year was a decisive one for freedom of expression in Russia and a "watershed moment" for Internet regulation (Lonkila et al., 2020). Control over the public sphere increased again in 2014 during the conflict with Ukraine and the occupation of Crimea. Yandex. News, in particular, found itself at the heart of a political controversy after being accused of partiality by the authorities for providing visibility to information that did not align with the official narrative. The site Pravda. ru wondered whether "Yandex lights a 'Maidan' in Russia?" (referring to the protests in Kiev that led to regime change in Ukraine).[2] The newspaper was outraged by the headlines chosen by the news aggregator and claimed that legal regulation of its activity was required. This led to the adoption in 2016 of a law on news aggregators that was designed to extend control of the media to such intermediaries and specifically targeted Yandex.News.[3] Those news aggregators that received over one million daily visitors became legally responsible for any content published in their results (and at risk of heavy fines in the event of violations), unless the selected media had been officially registered with Roskomnadzor. The law went into effect on January 1, 2017, whereupon all non-registered media (including dissenting voices such as Mediazona), as well as all foreign media (such as the BBC in Russian and exiled media such as Meduza), disappeared from both the Top 5 results presented on the Yandex homepage and Yandex.News. In sum, the aggregator may claim to be neutral and objective, but on the one hand, the authorities denounce its propensity to relay discontent and destabilize the political situation, while on the other hand, journalists, web professionals, and activists underline that its institutional framing requires it to promote a "loyal" agenda.

Its shortcomings have been made clear since Russia's invasion of Ukraine, as the last remaining independent media have gradually been shut down. In a post published on his Facebook page three days after the beginning of the war, Lev Gershenzon, former head of Yandex.News, stated:

> Now every day Russia's war against Ukraine is possible because there are no mass anti-war demonstrations in Russian cities. And they don't happen not only because of the danger of reprisals to those who do come out (huge admiration to all who do come out), but mainly because the vast majority of the population is unaware that Russian troops are in their fourth day of full-scale warfare. Leading this ignorance, along with television, is Yandex—a website and apps with a news bloc, 5 news, "on the home page." This news gets straight to people precisely because they do not come for it, but for some other reason: to find a product or the address of a pharmacy, to see the dollar exchange rate or the weather, etc. We once articulated that the task of this unit was to find out "if anything is wrong." So now it says: "no, there is no problem." […] Every hour and day that it works the way it does now is an endorsement of the war.[4]

The Yandex Rankings as a Gateway to the Algorithm and Its Transformations

Though it is difficult to investigate the algorithm itself, one can look at the output that the aggregator displays. During the month of June 2020, we conducted a quantitative analysis of the news selected by Yandex.News and presented as part of the Top 5 on the Yandex homepage.

[2] "Yandex 'razzhigaet' Majdan v Rossii?", Pravda, at http://www.pravda.ru/topic/yandex-617/.

[3] Federal Law № FZ-208, 23 June 2016.

[4] Lev Gershenzon Facebook page, February 27, 2022.

We carried out a systematic scraping of news: between June 1 and June 30, 2020, we automatically collected the Yandex.News rankings every two hours and listed a total of 3,011 references.[5] It appeared that, during this period, only 14 media outlets were cited in the Top 5—an extremely narrow sample considering the more than 7,000 sources listed in the Yandex.News database. We then extended the scraping to the period June–December 2020 and obtained the same results, with the same 14 media appearing in the Top 5 over this period. The data provide striking evidence of the concentration of information on Yandex.News with a few large media players: public press agencies, state-funded media, leading newspapers, and mainstream online publications (RIA Novosti, Gazeta.ru, Izvestia, RBK, Lenta.ru, RT in Russian, Kommersant, Regnum, Rossiiskaia Gazeta, TASS, Vesti.ru, Vedomosti, BFM.ru, and Interfax).

The over-representation of specific news publishers has also been demonstrated in the case of Google News (Schroeder and Kralemann, 2005; Haim et al., 2018), but not to such an extent. Our results from Yandex.News feature a much narrower range of publications than the findings of Nechushtai and Lewis (2019) in the case of Google News in the US, for instance. Although 14 outlets likewise dominated that aggregator, a long tail of other publications also figured in the results. Moreover, even if nuances can be detected between the 14 major media that dominate Yandex.News in terms of their editorial line, it is evident that in 2020, "officially sanctioned" media reached Yandex's heights more easily. Indeed, most of the 14 selected outlets are related to the Kremlin: they are either funded by the state directly or are privately owned by "loyalist" figures or entities and thus indirectly "managed" by the authorities.

The recent history of Yandex.News in Russia highlights how platform regulation can be leveraged to set up a form of "governance by algorithms" of the media and the public sphere. Initially presented as a technical means to "objectively" assess the diversity of online content, the aggregator sparked techno-political controversy in the 2010s: it was criticized by the authorities for promoting "unpatriotic" or "fake" news, while journalists, web professionals, and end users increasingly suspected that *inconvenient* truths would find it difficult to reach its top rankings. The adoption in 2016 of a law on news aggregators, which allowed only officially "registered" sources to be displayed by the service, clearly reflected an intention on the part of the authorities to domesticate the platform in order to limit the visibility of protests and discontent in the public sphere. This regulation took place in a complex digital ecosystem that articulates different levels of gatekeeping, including Yandex.News and other platforms, the telecommunications watchdog Roskomnadzor, as well as media outlets and journalists.

Yandex as a news recommender system abides by both legal and technical "codes of conduct" that help ensure that the information it promotes and amplifies remains in check. Although no outright censorship has yet been demonstrated at the level of Yandex.News, the aggregator appears to be an important cog in the machine of tightening control exerted by the authorities over the overall Russian media ecosystem. Until recently, however, governance by algorithms has remained imperfect and taken place in an intricate technical, political, legal, and economic context where national and international platforms have coexisted and competed.

Journalists and publishers could seek alternative channels to distribute information, relying on social media such as Telegram or Twitter. It remains to be seen how far this will still be possible as the war unfolds and the space for critical voices diminishes. Up until the beginning of the war, the Russian authorities justified their efforts to control the media agenda and to reassert their sovereignty over the public sphere by denouncing information framed as "unpatriotic," "fake" or otherwise problematic. Today, any dissenting views are being quelled, and the role of Yandex.News is at the heart of political concerns about the use of algorithms for warmongering.

About the Authors

Françoise Daucé is Professor at the School for Advanced Studies in the Social Sciences (EHESS), Paris, France and director of the Center for Russian, Caucasian and East-European Studies (CERCEC).

Benjamin Loveluck is Associate Professor at i3-SES, Telecom Paris, France.

References

- Bharat, K. (2006). "And now, News," *Google Official Blog*, 23 January 2006, https://googleblog.blogspot.com/2006/01/and-now-news.html

[5] We analyzed the code of the Yandex homepage and found that 10 news references were presented at any given time. We therefore set up a Node.js script to collect these 10 references every two hours: four references occupy places 1 to 4 of the Top 5, while the fifth place is likely occupied by the six other references on a rotating basis. The script uses two main Node libraries: Puppeteer for scraping and Mongoose for database registration. After manually analyzing the html code of the homepage and several other pages of the website, we wrote javascript code to scrape the content of the 10 top news (title, date, source name, source url, rank on the homepage). The data was then registered in a MongoDB database using the Mongoose library.

- Bozdag, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and Information Technology*, *15*(3): 209–227.
- Brake, D. R. (2017). The invisible hand of the unaccountable algorithm: how Google, Facebook and other tech companies are changing journalism. In J. Tong & S.-H. Lo (eds.), *Digital Technology and Journalism. An International Comparative Perspective*. Cham: Palgrave Macmillan, pp. 25–46.
- Bruns, A. (2019). *Are Filter Bubbles Real?* Cambridge: Polity Press.
- Christin, A. (2020). *Metrics at Work. Journalism and the Contested Meaning of Algorithms*. Princeton, NJ: Princeton University Press.
- Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly*, *80*(S1): 298–320.
- Fletcher, R., & Nielsen, R. K. (2018). Automated serendipity: the effect of using search engines on news repertoire balance and diversity. *Digital Journalism*, *6*(8): 976–989.
- Haim, M., Graefe, A., & Brosius, H.-B. (2018). Burst of the filter bubble? Effects of personalization on the diversity of Google News. *Digital Journalism*, *6*(3): 330–343.
- Lonkila, M., Shpakovskay, L., & Torchinsky, P. (2020). The occupation of Runet? The tightening state regulation of the Russian-language section of the internet. In M. Wijermars & K. Lehtisaari (eds.), *Freedom of Expression in Russia's New Mediasphere*. Abingdon and New York: Routledge, pp. 17–38.
- Nechushtai, E., & Lewis, S. C. (2019). What kind of news gatekeepers do we want machines to be? Filter bubbles, fragmentation, and the normative dimensions of algorithmic recommendations. *Computers in Human Behavior*, *90*: 298–307.
- Oates, S. (2013). *Revolution Stalled. The Political Limits of the Internet in the Post-Soviet Sphere*. Oxford and New York: Oxford University Press.
- Pariser, E. (2011). *The Filter Bubble. What the Internet Is Hiding from You*. New York: Penguin Press.
- Schroeder, R., & Kralemann, M. (2005). Journalism ex machina—Google News Germany and its news selection processes. *Journalism Studies*, *6*(2): 245–247.
- Soldatov, A., & Borogan, I. (2015). *The Red Web. The Kremlin's Wars on the Internet*. New York: PublicAffairs.
- Tufekci, Z. (2018). YouTube, the great radicalizer. *The New York Times*, 10 October 2018. https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html
- Wijermars, M. & Lehtisaari, K. eds. (2020). *Freedom of Expression in Russia's New Mediasphere*. Abingdon and New York: Routledge.

ABOUT THE RUSSIAN ANALYTICAL DIGEST

Editors: Stephen Aris, Matthias Neumann, Robert Orttung, Jeronim Perović, Heiko Pleines, Hans-Henning Schröder, Aglaya Snetkov

The Russian Analytical Digest is a bi-weekly internet publication jointly produced by the Research Centre for East European Studies [Forschungsstelle Osteuropa] at the University of Bremen (www.forschungsstelle.uni-bremen.de), the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology Zurich (ETH Zurich), the Center for Eastern European Studies at the University of Zurich (http://www.cees.uzh.ch), the Institute for European, Russian and Eurasian Studies at The George Washington University (https://ieres.elliott.gwu.edu), and the German Association for East European Studies (DGO). The Digest draws on contributions to the German-language Russland-Analysen (www.laender-analysen.de/russland), and the CSS analytical network on Russia and Eurasia (www.css.ethz.ch/en/publications/rad.html). The Russian Analytical Digest covers political, economic, and social developments in Russia and its regions, and looks at Russia's role in international relations.

To subscribe or unsubscribe to the Russian Analytical Digest, please visit our web page at http://www.css.ethz.ch/en/publications/rad.html

Research Centre for East European Studies at the University of Bremen
Founded in 1982, the Research Centre for East European Studies (Forschungsstelle Osteuropa) at the University of Bremen is dedicated to the interdisciplinary analysis of socialist and post-socialist developments in the countries of Central and Eastern Europe. The major focus is on the role of dissent, opposition and civil society in their historic, political, sociological and cultural dimensions.
With a unique archive on dissident culture under socialism and with an extensive collection of publications on Central and Eastern Europe, the Research Centre regularly hosts visiting scholars from all over the world.
One of the core missions of the institute is the dissemination of academic knowledge to the interested public. This includes regular e-mail newsletters covering current developments in Central and Eastern Europe.

The Center for Security Studies (CSS) at ETH Zurich
The Center for Security Studies (CSS) at ETH Zurich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching, and consultancy. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.
The CSS combines research and policy consultancy and, as such, functions as a bridge between academia and practice. It trains highly qualified junior researchers and serves as a point of contact and information for the interested public.

The Institute for European, Russian and Eurasian Studies, The Elliott School of International Affairs, The George Washington University
The Institute for European, Russian and Eurasian Studies is home to a Master's program in European and Eurasian Studies, faculty members from political science, history, economics, sociology, anthropology, language and literature, and other fields, visiting scholars from around the world, research associates, graduate student fellows, and a rich assortment of brown bag lunches, seminars, public lectures, and conferences.

The Center for Eastern European Studies (CEES) at the University of Zurich
The Center for Eastern European Studies (CEES) at the University of Zurich is a center of excellence for Russian, Eastern European and Eurasian studies. It offers expertise in research, teaching and consultancy. The CEES is the University's hub for interdisciplinary and contemporary studies of a vast region, comprising the former socialist states of Eastern Europe and the countries of the post-Soviet space. As an independent academic institution, the CEES provides expertise for decision makers in politics and in the field of the economy. It serves as a link between academia and practitioners and as a point of contact and reference for the media and the wider public.

Any opinions expressed in the Russian Analytical Digest are exclusively those of the authors.

Reprint possible with permission by the editors.
Editors: Stephen Aris, Matthias Neumann, Robert Orttung, Jeronim Perović, Heiko Pleines, Hans-Henning Schröder, Aglaya Snetkov
Layout: Cengiz Kibaroglu, Matthias Neumann, Michael Clemens
ISSN 1863-0421 © 2022 by Forschungsstelle Osteuropa an der Universität Bremen, Bremen and Center for Security Studies, Zürich
Research Centre for East European Studies at the University of Bremen • Country Analytical Digests • Klagenfurter Str. 8 • 28359 Bremen •Germany
Phone: +49 421-218-69600 • Telefax: +49 421-218-69607 • e-mail: laender-analysen@uni-bremen.de • Internet: www.css.ethz.ch/en/publications/rad.html