Russian Cyber Disinformation Campaigns and Possible Countermeasures

Michael R. Williams[1] and Neil C. Rowe[2][0000-0003-2612-0062]

Department of Computer Science, U.S. Naval Postgraduate School, USA

[1]mr_williams_dmb@yahoo.com, [2]ncrowe@nps.edu (correponding author)

Abstract. We discuss Russian cyber disinformation. Historical instances from the Cold War to today show consistent themes, motives, and strategies used by Russia in shaping narratives, manipulating public opinion, and undermining democratic processes. In examining social media, state-controlled media outlets, propaganda, and cyber operations, we see an intricate web of techniques to disseminate false information, amplify divisive narratives, and exploit vulnerabilities in target societies. Often the Russian source of this disinformation can be detected from the frequent use of their favorite keywords such as "election" and "fraud", "crime" and "Western", or "revolution" and "CIA". We examine possible countermeasures to combat Russian disinformation, such as fact checking, media-literacy programs, and sharing of information. We also must bolster cybersecurity, promote transparency in social-media platforms, and develop comprehensive legislation to address the multifaceted nature of disinformation.

Keywords: Russia, Disinformation, Cyber, Social Media, Influence, Propaganda, Cybersecurity, Deception.

This paper appeared in the Proceedings of the 24th International Conference on Security and Management, Las Vegas, NV, US, July 2024.

1 Introduction

As technology advances and the distribution of news and information becomes easier, manipulating news and information has become easier too. This creates opportunities for national adversaries to gain an advantage. This includes both misinformation (incorrect or misleading information) and disinformation (deceptive information intentionally spread to influence public opinion or hide the truth). Both can be part of an "influence operation" for political or military goals, often to "weaponize" information against an enemy. They try to manipulate public opinion, disrupt activities, or destroy entities. The psychological effects are fear, confusion, and cynicism. For example, in 2020, COVID-19 vaccine rumors and conspiracy theories ranged from "vaccines don't work" to "the government is putting microchips in vaccines to track you" [16]. On social media such as Facebook and Twitter, campaigns from Russia [22] discouraged people from getting vaccinated, contributing to the pandemic. Disinformation can overwhelm its audience with dramatic fake statistics, fake correlations, and emotional stories. Users on social media that “liked” and “shared” this content helped disperse these false stories. Healthcare professionals complained that they not only had to fight COVID-19 but also false or misleading information [26].

Russia has run many online influence and disinformation campaigns targeting other countries. Since 2013, the Russian government has used its Internet Research Agency (IRA) to spread “dezinformatsiya” or disinformation [8]. Their disinformation campaigns are coordinated operations that contrive false, misleading, or manipulated information to destabilize their enemies. Technological advancements have greatly helped Russia’s campaigns.

Even in 1923 the Russian government had a “special disinformation office” to manage “false information with the intention to deceive public opinion” [56], a kind of espionage. These campaigns have targeted race, ethics, and political issues, including elections, for a century [42]. As an example, in 1982 an English newspaper in India published an article titled "Operation INFEKTION," which said that the United States created and spread the HIV/AIDS virus [57]. It offered an easy excuse to mistrust the U.S. government, which advanced Russian interests. It took U.S. media six years to detect the Operation INFEKTION article. Today, similar stories can circulate on the Internet rapidly and reach millions of readers. Malicious software such as botnet technology, password crackers, distributed denial of service, and “deep fakes” [13] are now used by Russia to amplify effects in influence campaigns. Recently the Mueller Report revealed Russia’s “bots” (automated Internet processes), “trolls” (online provocateurs), social media, impersonation, and other technical methods to interfere with the 2016 U. S. Presidential election [50]. However, the report was three years after the election, too late to make a difference.

Much of this disinformation is offered by impersonators who are difficult to unmask. This is troubling given that nearly 55% of adult Americans receive daily news from uncurated social media like Twitter, Facebook, Instagram, YouTube, Reddit, and Snapchat [63]. Also, legitimate news sources can offer disinformation when they have been victims of untrustworthy sources or unauthorized modification of their sites, and deepfake technology can create especially convincing disinformation. Russia has by far the largest disinformation campaigns of any country; China and the United States focus their espionage on collecting secrets instead.

Section 2 discusses how influence campaigns are constructed and implemented. Section 3 describes how technological advancements aid Russia's campaigns. Section 4 suggests ways to discover and debunk Russian disinformation and the importance of media literacy. Section 5 gives a final assessment. More details are in [78].

2 Influence Concepts

2.1 Information Operations

It helps to distinguish several techniques:

- Propaganda: A story told to sway people's political or social ideas [20]. For example, the Taliban used propaganda in Afghanistan for their ideology, recruiting fighters, and undermining the government [76].
- Misinformation: False information spread for entertainment or other purposes not intended to influence. False conspiracy theories or hoaxes have been disseminated through social media without concrete evidence. Misinformation is common in social media because of the ease of distributing it and the rarity of checking it [3].
- Disinformation: Information that the disseminator knows to be false. Examples are spreading fake news through media outlets and tampering with private messages. Disinformation is more powerful than misinformation.
- Statistics: Counts and averages such as the number of people affected by a problem, the prevalence of a particular disease, or the economic effect of a policy [69].
- Likely facts: Quotes and opinions from experts in relevant fields. Expert opinion from accredited doctors combatted misinformation during the COVID-19 pandemic.
- Historical facts: The history of an issue or topic to provide context.
- Scientific evidence: Scientific studies and research can support arguments and claims.

2.2 Influence

Influence is a key concept in business marketing. Its tactics can be used for disinformation-based influence operations [44]:

- Understand the beliefs, values, motivations, and decision-making of the target audience.
- Build trust and credibility: Use credible sources, testimonials, and consistent messaging.
- Obfuscate, confuse, disrupt, or diminish truthful reporting and messaging. Russia does this frequently [55].
- Appeal to emotions: Use images, stories, and symbols that resonate with the target audience. In the war between Russia and Ukraine, Russians have frequently posted images of Russian soldiers and vehicles on the Internet.
- Use a multi-channel approach: Use a variety of traditional and digital media to reach a wide audience.
- Monitor and adapt continually: Adjust the operation to the situation and feedback from the target audience.
- Encourage groupthink: Get people to make irrational or dysfunctional decisions conforming to a group [38].

3 RUSSIAN INFLUENCE METHODS

3.1 Campaigns

Russia is experienced in disinformation. It does not exclusively focus on politics or on one side of an issue, but exploits all sides of any topic that can disrupt a society [31].

However, the CIA did note Russian election interference in the 1964, 1968, and 1984 U.S. presidential elections [40], and found the Russians discouraged votes for candidates that opposed communist politics and practices, then generally Republicans. The CIA estimated that the Soviets spent $3 billion annually on disinformation campaigns in this period [74]. Propaganda efforts decreased after the disintegration of the Soviet Union but continued to promote the regime in Russia. The U.S. Active Measure Working Group acted to debunk Russian disinformation attempts then.

To increase confusion after the terrorist attack on September 11, 2001, Russian media promoted conspiracy theories suggesting that the attack was coordinated by the United States [37]. Despite lack of evidence, they became headlines in some U.S. newspapers. After 2001, Russia mainly targeted former Soviet states, the National Atlantic Treaty Organization, and the European Union [67]. Russian disinformation campaigns occurred against Europe, Sweden, Ukraine, Estonia, and others, and campaigns became bolder. For instance, when a Malaysian aircraft was shot down over Ukraine in 2014 [66], Russian actors attributed it to a Ukrainian fighter jet although later it was confirmed to be a Russian surface-to-air-missile.

Russian disinformation often exploits tensions in a society. For example, between 2015 and 2017, a campaign using at least 13 accounts created over 129 Facebook events [53]. 300,000 people viewed the event invitations, and 65,000 said that they would attend. The events were designed to cause confrontations; for instance, two rallies with opposite points of view on immigrants (“Heart of Texas” and “United Muslims of America”) were called by Russian agents on the same day for the same location in Houston, Texas.

3.2 Favorite Disinformation Topics

Russia has several favorite false narratives that it repeats in its disinformation and propaganda [73]. Most are easy to detect from the use of certain limited sets of keywords. Five commonly heard ones are:

1. Russia is a victim of other countries. Disinformation frequently depicts Russia as unfairly targeted, and rationalizes their forceful actions as defenses to the conduct of the United States and its allies. They accuse the United States of "Russophobia" [49] and label anyone questioning Russian activities as xenophobic and Russophobic. This tactic was often used after the 2014 invasion of Ukraine.
2. Distortion of history to make Russia look better, as in the 2022 Russian invasion of Ukraine [5]. Early in the conflict, the Russian government denied involvement, and it claimed that the Ukrainian government caused the unrest in eastern Ukraine. However, once Russian military personnel and equipment were clearly seen in the region, Russia inconsistently claimed Ukraine was taken over by Nazis, and they intervened to rescue it.
3. The collapse of Western civilization is imminent. Russia claims that Western civilization is “rotting” and “decadent”, has forsaken "traditional values" because it supports equality and diversity [52] and is crime-ridden.

4. The U.S. creates revolutions to destabilize countries. Russia has accused the United States of inciting revolutions in Kazakhstan, Moldova, the country of Georgia, the Kyrgyz Republic, Ukraine, and other countries in the Middle East and Africa. Russia doubts the legitimacy of popular movements that are pro-democracy, pro-reform, or not in their geopolitical interests, and asserts that the United States secretly supports them [21]. Russia rejects that other nations have agency, dignity, and the right to speak for themselves.
5. Alternative realities. When reality is inconvenient, Russia creates alternative realities and sows uncertainty about reality. Contradicting state-funded storylines can confuse targets and deter responses [29]. Russia did this to shift attention from its participation in the downing of Malaysia Airlines Flight 17, and in the invasion and occupation of Georgia in 2008 [66]. It also often claims foreign elections are fraudulent when its favored candidates lose.

3.3 Disinformation Dissemination

Russia uses many actors for disinformation, including both governmental and allegedly non-governmental agents [43]. A non-governmental actor allows Russia to deny involvement; examples are cyber terrorists, non-governmental organizations, hackers, and hacktivists [68]. Hacktivists use anonymous cyber proxies to do cyber civil disobedience for political causes. Russia posts instructions for hacktivists on the Internet; for instance, instructions for ICMP, ping, and TCP SYNC floods were provided in 2007 to allow amateurs to do denial of service against Estonia [34]. Russia also has non-governmental organizations propagate disinformation. Such organizations appear less biased when they participate in "soft" tasks like education, history, and cultural exchanges [46]. The Ghanaian organization "Eliminating Barriers to the Liberation of Africa", which supported Internet activism and human rights, was linked to the Russian IRA [77]. Despite its name, it tried to influence the 2016 United States Presidential election by focusing on persecution in black neighborhoods, police brutality, and civil rights. Opportunists in many countries endorse disinformation for political purposes despite knowing it is false [62], such as the U.S. public officials who claimed fraud in the 2020 U.S. election despite no evidence found in over 60 investigations [14][30]. Similarly, violent crime in the U.S. has been decreasing since 1990 [72], so the U.S. is getting safer despite Russian disinformation repeated by U.S. politicians.

Russia has an assembly line for disinformation. Today, deepfakes generated by artificial neural networks are increasingly automating disinformation production [13]. Much of it is done by the Russian IRA at a highly guarded structure known as the "Troll Factory" in St. Petersburg, Russia [4]. Employees create and distribute products on the Internet, operating like a factory with specialized sections such as those fostering societal animosity and undermining political authority, or extremist positions like those of QAnon. The U.S. Justice Department charged IRA personnel in February 2018 with interfering with the 2016 presidential elections by using trolls on social-networking sites.

Since anyone can create a Web site, discussion board, or social-media account, these are good places to disseminate disinformation. Twitter (now X), Facebook (now Meta), and Instagram social-media platforms have often posted Russian disinformation [79]. Facebook, for instance, had 2.2 billion active users in 2023 and offered easy signup by requiring only a name, email address, and birthday. This can be increased by implanting malware on networks. Furthermore, user identities are unverified, so malicious actors can create unlimited accounts to post disinformation. Facebook deleted over three billion fake accounts in 2019 [62], but only after the 2016 election. Twitter allows users up to 2400 posts daily, which enables using automated accounts (“bots”) for posting. Twitter says it denies over 500,000 new user requests from bots daily with CAPTCHA authorization, a weak form of verification [69]. However, human-assisted bots can now bypass authentication efforts effectively [17]. Bots can generate followers, likes, and reposts to make themselves look credible and popular. Twitter auditing in 2018 found that 60% of Donald Trump’s Twitter followers were bots [28]. After the 2016 election, Twitter published a list of over 10 million fake accounts to show the public the reach of Russian disinformation [69]. However, many current X users are still undetected bots.

The Russian government also broadcasts “official” disinformation through domestic media platforms such as Sputnik and Russia Today. These often criticize independent media institutions. Much of their disinformation is lies or half-truths about espionage, terrorism, and national elections.

3.4 More about Election and Government Interference

Russia has been trying to influence elections worldwide since the 17th century [58]. They do not consistently support political parties, but support their best opportunity. In the 1964 U.S. presidential election, the Soviet Union saw the Republican candidate Goldwater as a threat [40] due to his anti-Soviet beliefs. Soviet and Czechoslovak intelligence agencies launched a disinformation campaign portraying Goldwater as a racist and mentally unfit for office. This campaign sent disinformation documents to many journalists.

Russian manipulation was seen even more in the 2016 U.S. presidential election [50], in a campaign planned years in advance. In 2014, Russian agents in the US to create social-media accounts on various political issues, often by impersonation. They amassed hundreds of thousands of likes and followers, and earned credibility and reach by getting reposted and interacting with supporters of candidates they favored to reach a wider audience. Fake images were created such as those showing Presidential candidate Clinton shaking hands with the Al Qaeda leader, which were widely distributed across social-networking sites [39]. Russian actors also used spear phishing against a Clinton campaign member, John Podesta, stole his email, and released it through Wikileaks, an anti-secrecy organization used in some Russian disinformation campaigns [25]. Another disinformation campaign (“Pizzagate”), circulated using botnets traced to St. Petersburg, alleged that a pizza parlor was a child sex-trafficking ring supervised by Clinton [35]. This caused a gunman to drive 300 miles to free victims he believed to be trapped in a nonexistent basement.

In the 2020 presidential election, Russian agents used more fake social-media accounts and attempted to hack into email servers and state voting systems [12]. This time, however, the U.S. government and social-media platforms were more aware of Russian tactics and stopped many attacks [27] by locking down and actively monitoring servers, and removing thousands of fake accounts [22]. However, this was only a few since Facebook has 2.2 billion daily users and Instagram has over a billion. Social-media platforms now use artificial intelligence to identify fake accounts and disinformation [62], but it is not easy. Also, sites may not want to remove fake accounts that earn them money.

The U.S. is not the only victim of Russian election meddling [9]. In March 2018, the Dutch government claimed that Russian hackers had tried to get into its systems, part of the Cozy Bear group associated with the Russian intelligence agency FSB. The French 2017 election also saw hacking attempts and disinformation campaigns [36]. The campaign of Emmanuel Macron was targeted by a cyberattack just two days before the final round of presidential elections, an attack later attributed to Russia. It used phishing emails to target campaign staff, and stole their emails. Text was then altered to create false narratives about the campaign. After this attack, the French government established a task force CNPPUE which monitored social media and other online platforms for signs of disinformation about the election. They also worked with political parties and candidates to improve online security, and provided training on detecting and preventing disinformation.

In 2019, Russia was accused of spreading false information, propaganda, manipulated media narratives, and cyberattacks to undermine the legitimacy of Ukraine's government [71]. These attacks tried to disrupt Ukraine's political and electoral processes and aid pro-Russian candidates. In 2022, an obvious Russian deepfake video was released showing Ukrainian President Zelensky urging surrender to Russia [60]. Similar Russian activities were seen in the 2008 invasion of Georgia. Georgia was subject to cyberattacks that disrupted its government and communication systems [23]; attacks hit government websites, news agencies, and banks. The apparent goal was to create confusion, manipulate public opinion, and damage Georgia's credibility; for instance, false information portrayed Georgia as the aggressor.

4 COUNTERMEASURES AND RECOMMENDATIONS

Russian influence campaigns are complex and multifaceted, and countering them requires a multi-pronged approach [7]. Campaigns do vary with the target. For a U. S. election, they try to divide conservatives and liberals; for neighboring states, they try to divide ethnic Russian populations from others [33].

4.1 Educating the Public

One way to counter Russian influence campaigns is to educate the public about their tactics, motivations, and goals [47]. While this can be effective, confirmation bias means people tend to more easily accept new information that supports what they already believe, and reject information that goes against their beliefs [51]. Russian campaigns frequently exploit confirmation bias for the groups they target [24]. With sophisticated algorithms and machine learning, Russians can identify their target audience's preferences, values, and beliefs, and tailor their messages to those biases. This can create a reinforcing loop in which people are more receptive to similar propaganda and disinformation. Nonetheless, the public can be educated about disinformation [1]. Some methods are:

- Develop educational materials about disinformation campaigns to describe tactics such as false information, misleading headlines, manipulation of images or videos, fake social-media accounts, and bots and trolls. Educational materials can be distributed through social media, news outlets, and schools.
- Run public-awareness initiatives through social media, public events, and advertising. Civil-society organizations such advocacy groups can help. The U.S. cybersecurity CISA has a program disseminating correct information about election security [18].
- Public figures must be knowledgeable about identifying and countering disinformation campaigns. Laws and regulations can reduce the spread of false information and limit its impact. Russian disinformation is so common that it is also important for media to identify when it has been disproved, as with the Hunter Biden laptop whose contents were initially blamed by Democrats on Russian disinformation [11].
- Social-media companies can promote media literacy by identifying fake news, propaganda, and disinformation, often by recognizing abusive language. They can remove such content by policies [48]. Many favorite Russian themes mentioned in section III.B are easily identified by keyword search, as by “election” and “fraud”, “degenerate” and “West”, or “CIA” and “revolution”; they can also be identified by page-ranking algorithms [3]. These clues are often easy to check, so social media companies have no excuse for not policing them.
- Estimating influence can be done by causal inference [61] based on the relationships between users and their actions in a social-media network. One can rank users to find the most influential.
- Machine learning and natural-language processing on social-network data can identify clusters of users who spread false information [2]. Disinformation campaigns are often well coordinated, with a few key influencers spreading the most lies [41].
- Network monitoring can trace disinformation sources through geolocation of addresses or image metadata. Despite attempts to hide this information by criminals and others with malicious intentions, increasing international cooperation due to the Convention on Cybercrime is improving traceability of Internet data.
- If malware is associated with disinformation, it can be traced independently. The malware’s code may have signatures that help identify its source. Signatures can be traced in network traffic and may allow matching to known malware in databases of antimalware resources.

A more general solution is the improvement of media literacy in the public: good methods for accessing, analyzing, evaluating, and creating of media [32]. It involves understanding how media works, including how news is reported, how images and videos are created and edited, and how messages are conveyed through different media channels [65]. By understanding the consequences of sharing false or misleading information, people can become more cautious about what they share online and more likely to verify the accuracy of information before sharing it. A related concept of "digital readiness" refers to a person's or a community's skill in using digital technologies, including Internet accessibility, digital devices, and digital literacy. People and societies lacking digital readiness may be more vulnerable to disinformation because they may not understand the technology.

4.2 Increasing Transparency and Truthfulness

Another way to combat disinformation is for governments and social media to mandate increased transparency in messages by requiring disclosure of the authors and sources of funding, especially for political ads [10]. Fact-checking organizations can verify the accuracy of claims and identify misleading or false ones. On Internet pages, links to fact checking can be added automatically. Independent media can help promote transparency and provide diverse viewpoints to reduce disinformation's influence. For instance, Radio Free Europe/Radio Liberty counters Russian influence campaigns by providing independent news and information where the government censors or heavily controls the media. It can help by fact-based reporting [64], investigative journalism, language expertise (news and information in local languages), and partner with local media to support independent journalism.

Although the U.S. Constitution First Amendment guarantees a right to freedom of speech, the Supreme Court has ruled that the Constitution does not protect defamation, perjury, fraudulent schemes for financial gain, false torts, and lies that cause significant emotional harm [75]. It can be challenging and expensive to refute false claims legally; even if one wins in court, lies and disinformation may have already spread [19]. Nevertheless, independent fact-checking organizations that debunk false claims can encourage people to verify the information before accepting it as true [59]. Media platforms can help by providing ways for users to report false or misleading content.

When evidence of foreign political interference is found, the perpetrators should face consequences. For instance, after the 2016 U.S. presidential elections, actions were taken against Russia [80]. The U.S. government imposed economic sanctions on Russian entities and people involved in the interference, including the IRA. The U.S. Justice Department indicted 13 Russians and three Russian companies associated with the IRA, expelled 60 Russian diplomats in 2018, and closed a Russian consulate. In the 2020 election, evidence showed that public exposure of Russian techniques reduced their effect [45].

4.3 Strengthening Cybersecurity

To prevent cyberattacks aiding the placement and dissemination of disinformation, we must strengthen cybersecurity measures for political campaigns, government agencies, and critical infrastructure [6]. Firewalls, intrusion-detection systems, and antivirus software can significantly reduce unauthorized access to systems which are a good base for spreading disinformation through fake accounts or where secrets can be stolen for political manipulation. Governments and political organizations can invest in more robust cybersecurity defenses, including encryption and multi-factor authentication, to better control access. Organizations can provide cybersecurity training to help employees recognize and respond to phishing attempts, malware, and other cyberattacks. Regular security assessments can identify vulnerabilities in systems and networks, and fix them before they are exploited [15].

5 CONCLUSIONS

Russian disinformation poses major challenges to global stability, democratic processes, and information integrity. From social-media manipulation to creating fake news outlets and weaponizing hacked information, Russia has shown much adaptability. However, their targets for creating divisiveness can often be predicted based on their history.

To combat this threat, a multi-faceted approach is essential. First, monitoring elections is a high priority in safeguarding democratic processes. Establishing independent oversight bodies and deploying software tools can detect and counter disinformation efforts. While the U.S. did bolster its monitoring and cybersecurity for the 2020 elections, it must continue this consistently. Some fakes can be detected using machine learning from artificial intelligence [13].

International cooperation can address the transnational nature of Russian disinformation campaigns. Governments, intelligence agencies, and civil society organizations should share intelligence, exchange best practices, and develop coordinated responses. Technological advancements in improved algorithms, machine-learning models, and artificial intelligence can help identify deceptive content. Collaboration between technology companies, researchers, and governments is necessary to develop and implement innovative solutions. Research should also develop media-literacy programs, fact-checking organizations, transparency measures, and regulatory frameworks.

Acknowledgments. The views in this paper are those of the authors and do not represent those of the U.S. Government. Thanks to Shannon Houck for reviewing an earlier draft.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Abrams, Z.: Controlling the spread of misinformation. Monitor on Psychology, **52**(2), 44 (March 1, 2021)
2. Alizadeh, M., Shapiro, J., Butain, C., Tucker, J.: Content-based features predict social media influence operations. Science Advances, **6**(30) (July 22, 2020)
3. Allen, J.: Misinformation amplification analysis and tracking dashboard. Integrity Institute, https://integrityinstitute.org/blog/misinformation-amplification-tracking-dashboard (March 13, 2023)

4. Aro, J.: The cyberspace war: Propaganda and trolling as warfare tools. European View, **15**(1), 121-132 (2016)
5. Beauchamp, Z.: Why Is Russia invading Ukraine? Vox, https://www.vox.com/2022/2/24/22948944/putin-ukraine-nazi-russia-speech-declare-war (February 24, 2022)
6. Belfer Center for Science and International Affairs of Harvard Kennedy School: Cybersecurity campaign playbook. https://www.belfercenter.org/publication/cybersecurity-campaign-playbook (November 2017)
7. Bodine-Baron, E.: Countering Russian social media influence. RAND Corporation, Report RR2740 (November 1, 2018)
8. Boghardt, T.: Soviet bloc intelligence and its AIDS disinformation campaign. Studies in Intelligence, **53**(4), 1–24 (2019)
9. Brattberg, E., Maurer, T.: Russian election interference: Europe's counter to fake news and cyber attacks. Carnegie Endowment for International Peace, Report CP333 (May 2018)
10. Brennen, J., Perault, M.: How to increase transparency for political ads on social media. Brookings Institute, https://www.brookings.edu/blog/techtank/2021/03/19/how-to-increase-transparency-for-political-ads-on-social-media/ (March 9, 2022)
11. Broadwater, L.: Officials who cast doubt on Hunter Biden laptop face questions. The New York Times, https://www.nytimes.com/2023/05/16/us/politics/republicans-hunter-bidenlaptop.html (May 16, 2023)
12. Bushwick, S.: Russia's information war is being waged on social media platforms. Scientific American, www.scientificamerican.com/article/russia-is-having-less-success-at-spreading-social-media-disinformation/ (March 8, 2022)
13. Byman, D., Gao, C., Meserole, C., Subrahmanian, V.: Deepfakes and international conflict. The Brookings Institution, Foreign Policy at Brookings report, https://www.brookings.edu (January 2023)
14. Campaign Legal Center: Results of lawsuits regarding the 2020 elections. https://campaignlegal.org/results-lawsuits-regarding-2020-elections, last accessed May 28, 2024
15. Cavelty, M., Wenger, A.: Cyber security meets security politics: complex technology, fragmented politics, and networked science. Contemporary Security Policy, **41**(1), 5–32 (2020)
16. CDC.gov: Bust myths and learn the facts about COVID-19 vaccines. https://cdc.gov/oronavirus/2019=ncov/vaccines/facts.html, last accessed September 27, 2023
17. Chu, Z., Wang, H., and Jajodia, S.: Detecting automation of Twitter accounts: Are you a human, bot, or cyborg? IEEE Transactions on Dependable and Secure Computing, **9**(6), 811-824 (Nov.-Dec. 2012)
18. CISA [U. S. Cybersecurity and Infrastructure Security Agency]: Election security rumor vs. reality. https://www.cisa.gov/rumor-vs-reality, last accessed November 24, 2022
19. CITS: Protecting ourselves from fake news: fact-checkers and their limitations. https://cits.ucsb.edu/fake-news/protecting-ourselves-fact, last accessed May 27, 2024
20. Cohen, R.: Combating foreign disinformation on social media: study overview and conclusions. RAND Corporation, report R4273 https://www.rand.org/pubs/research_reports/RR4373z1.html (July 19, 2021)
21. Cordesman, A.: Russia and the 'color revolution'. Center for Strategic and International Studies, https://www.csis.org/analysis/russia-and-color-revolution (September 21, 2022)
22. Culliford, E.: Facebook removes Russian network that targeted influencers to peddle anti-vax messages. Reuters. https://www.reuters.com/technology/facebook-removes-russian-network-that-targeted-influencers-peddle-anti-vax-2021-08-10/ (August 11, 2021)

23. Dickinson, P.: The 2008 Russo-Georgian war: Putin's green light. Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/the-2008-russo-georgian-war-putins-green-light/ (August 7, 2021)
24. Eckel, M.: Five things to know about the U.S. intelligence report on Russian election interference. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/five-things-us-intelligence-report-russian-election-interference/31156225.html (December 8, 2022)
25. Edmondson, C.: State Dept. inquiry into Clinton emails finds no deliberate mishandling of information. The New York Times (October 18, 2019)
26. Eysenbach, G.: How to fight an infodemic: the four pillars of infodemic management. Journal of Medical Internet Research, **22**(6) (2020)
27. Facebook.com: Removing more coordinated inauthentic behavior from Russia. Meta.com. https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/ (March 24, 2021)
28. Fishkin, R: We analyzed every Twitter account following Donald Trump. SparkToro.com. https://sparktoro.com/blog/we-analyzed-every-twitter-account-following-donald-trump-61-are-bots-spam-inactive-or-propaganda/ (October 8, 2018)
29. Gamberini, S.: Social media weaponization: the biohazard of Russian disinformation campaigns. Center for the Study of Weapons of Mass Destruction. https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2422660/social-media-weaponization-the-biohazard-of-russian-disinformation-campaigns (November 19, 2020)
30. Goins, F., Garretson, L.: Litigation in the 2020 election. American Bar Association. https://www.americanbar.org/groups/public_interest/election_law/litigation, last accessed October 27, 2022
31. Graff, G.: Russian trolls are still playing both sides. Wired Security. (October 19, 2018)
32. Guess, A., Lerner, A., Lyons, M., Montgomery, B., Nyhan, J., Reifler, J., Sircar, N.: A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. Proceedings of the National Academy of Sciences of the U. S., **117**(27) 15536–15545 (2020)
33. Helmus, T.: Russian social media influence: understanding Russian propaganda in Eastern Europe. RAND Corporation, report RR2237 (April 12, 2018)
34. Herzog, S.: "Revisiting the Estonian cyber attacks: digital threats and multinational responses. Journal of Strategic Security, **4**(2) 49-60 (2011)
35. Horton, A.: After truth: how ordinary people are "radicalized" by fake news. The Guardian. (March 30, 2020)
36. Hosenball, M., Menn, J.: Experts say automated accounts sharing fake news ahead of French election. Reuters.com. https://www.reuters.com/article/us-france-election-socialmedia-idUSKBN17M31G (April 21, 2017)
37. Hotchkiss, M.: Russian information warfare and 9/11 conspiracism: when fake news meets false prophecy. In: Developments in Information Security and Cybernetic Wars, Hershey, PA, US: IGI Global, 236-266 (2019)
38. Janis, I.: Groupthink: psychological studies of policy decisions and fiascoes, 2nd ed. Cengage Learning (1982)
39. Jensen, B.: How the Taliban did it: inside the "operational art" of its military victory. Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/how-the-taliban-did-it-inside-the-operational-art-of-its-military-victory (August 16, 2021)
40. Jones, S.: Russian meddling in the United States: the historical context of the Mueller Report. Center for Strategic and International Studies, csis.org, https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report?fbclid=IwAR00UP-3tyqB-N9PlYKeNGqhpS1J6W-8DbS-CgQ3EE4P7EBn3VDxaDomDtw (March 27, 2019)

41. Juul, J., Ugander, J.: Comparing information diffusion mechanisms by matching on cascade size. Proceedings of the National Academy of Sciences, **118(**46), e2100786117 (November 8, 2021)
42. Kennan, G.: George Kennan's "Long Telegram". Wilson Center Digital Archive, wilsoncenter.org, https://digitalarchive.wilsoncenter.org/document/george-kennans_long telegram (1946)
43. Klimburg, A.: Mobilising cyber power. Survival, **53**(1), 41-60 (January 2011)
44. Larson, E., Darilek, R., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L., Thurston, C.: Foundations of Effective Influence Operations. A Framework for Enhancing Army Capabilities. USA: RAND Corporation (2009)
45. Levin, D: Is sunlight the best counterintelligence technique? The effectiveness of covert operation exposure in blunting the Russian intervention in the 2020 U.S. election. Intelligence and National Security, **38**(5), 816-834 (2023)
46. Linvill, D., Warren, P.: Troll factories: manufacturing specialized disinformation on Twitter. Political Communication, **37**(4), 447-467 (2020)
47. Matthews, M.: Understanding and Defending against Russia's Malign and Subversive Information Efforts in Europe. RAND Corporation, report RR3160 (August 16, 2021)
48. Miller, M.: Facebook removes hundreds of accounts linked to Russian agencies ahead of election. The Hill, thehill.com (September 24, 2020)
49. Morson, G.: What is 'Russophobia?' Commentary (November 2023)
50. Mueller, R.: Report on the Investigation into Russian Interference in the 2016 Presidential Election. U.S. Department of Justice. https://justice.gov/archives/sco/file/1373816/dl (March 2019)
51. Nickerson, R.: Confirmation bias: A ubiquitous phenomenon in many guises. Review of General Psychology, **2**(2) (June 1998)
52. Novitskaya, A., Sperling, V., Sundstrom, L., Johnson, J.: Unpacking "traditional values" in Russia's conservative turn: gender, sexuality and the Soviet legacy. Europe-Asia Studies, **76**(2) 173-197 (July 13, 2024)
53. O'Sullivan, D.: Russian trolls created Facebook events seen by more than 300,000 users. Money.cnn.com. https://money.cnn.com/2018/01/26/media/russia-trolls-facebook-events/index.html (January 26, 2018)
54. Pacepa, I., Rychlak, R.: Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism. WND Books (2013).
55. Paul, C., Matthews, M.: The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation, Perspective Report PE-198-OSD (2016)
56. Prokhorov, A. (ed.): Great Soviet Encyclopedia: A Translation of the Third Edition. London, UK: Macmillan (1973)
57. Shevchenko, N.: How the KGB convinced the world that AIDS was a Pentagon invention. Russia Beyond. https://www.rbth.com/history/333296-kgb-aids-operation-infektion-pentagon (2023)
58. Shimer, D.: Rigged: America, Russia, and One Hundred Years of Covert Electoral Interference USA: Knopf (2020)
59. Silverman, C. (ed.), Verification Handbook 3: For Disinformation and Media Manipulation. Netherlands: European Journalism Center (2024)
60. Simonite, T.: A Zelensky fake was quickly defeated; the next one might not be. Wired Business (March 17, 2022)

61. Smith, S., Kao, E., Shah, D., Simek, O., Rubin, D.: Influence estimation on social media networks using causal inference. In: IEEE Symposium on Software Performance (April 11, 2018)
62. Stengel, R.: Information Wars: How We Lost the Global Battle against Disinformation and What We Can Do about It. USA: Atlantic Monthly Press (2019)
63. Suciu, P.: More Americans are getting their news from social media. Forbes (October 11, 2019)
64. Sullivan, M.: The Kremlin tries to stifle Radio Free Europe — and its audience surges. Washington Post (March 27, 2022)
65. Terrell.com: 50 Challenging Activities to Promote Digital Media Literacy in Students. https://www.teachthought.com/literacy/digital-media-literacy/ (2022)
66. Toal, G., O'Loughlin, J.: Why did MH17 crash? Geopolitics, **23**(4) 882-896 (2018)
67. Topor, L., Tabachnik, A.: Russian cyber information warfare. Journal of Advanced Military Studies, **12**(1) (December 1, 2021)
68. Traynor, I.: Russia accused of unleashing cyberwar to disable Estonia. The Guardian, **17**(5) (2007)
69. Turcilo, L., Obrenovic, M.: Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy. Heinrich Boll Stiftung (2020)
70. Twitter: Disclosing networks of state-linked information operations we've removed. https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html (June 12, 2020)
71. Ukraine Election Task Force: Foreign Interference in Ukraine's Election. Atlantic Council. https://www.atlanticcouncil.org (May 15, 2019)
72. USAfacts.org: Is the criminal justice system working? Is the country getting safer? https://usafacts.org/state-of-the-union/crime-justice (2024)
73. U.S. Department of State: "Russia's top five persistent disinformation narratives. https://www.state.gov/russias-top-five-persistent-disinformation-narratives/ (January 21, 2022)
74. U.S. House, 96th Congress, Second Session: Hearing before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence (February 6, 1960)
75. Volokh, E.: When are lies constitutionally protected? Knight First Amendment Institute. https://knightcolumbia.org/content/when-are-lies-constitutionally-protected#:~:text=Punishable%20Lies,distress%20are%20all%20constitutionally%20unprotected (October 19, 2022)
76. Walla, K.: Before the Taliban took Afghanistan, it took the Internet. Atlantic Council. (August 26, 2022)
77. Ward, C.: How Russian meddling is back before 2020 vote. Cable News Network. https://2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html (April 11, 2020)
78. Williams, M.: Russian Disinformation Campaigns in the United States and Possible Countermeasures. M. S. thesis, U.S. Naval Postgraduate School (June 2023)
79. Woolley, S.: Automating power: social bot interference in global politics. First Monday, **21**(4) (2016)
80. Yourish, K., Buchanan, L., Watkins, D.: A timeline showing the full scale of Russia's unprecedented interference in the 2016 election, and its aftermath. New York Times (September 20, 2018)