Russian Disinformation Tactics Fueling the Rise of Nationalism: An Analysis of Western Response

Disinformation is not merely a weapon of war; it is a tool for shaping societies. Following the annexation of Crimea in 2014, Russia's disinformation campaigns surged, fueled by a government-backed wave of nationalism. These campaigns have had dual purposes: solidifying domestic loyalty to the Kremlin and spreading discord among adversaries. By exploiting nationalist narratives, disinformation has become a key mechanism for the Russian state to control public perception and project power abroad. This paper investigates the intersection of Russian nationalism and disinformation tactics, analyzing their profound societal impacts and the digital challenges they pose to the West.

Following the annexation of Crimea in 2014, nationalism in Russia became increasingly entwined with a sharp rise in anti-Western sentiment the Kremlin actively cultivated as a cornerstone for its domestic and foreign policy. This shift was not an organic public reaction but a deliberate strategy employed by the Russian state to consolidate national unity and to justify aggressive policies both at home and abroad. Notably, Russia's 2012 'foreign agent' law expanded significantly after Crimea's annexation to label NGO's and independent media as foreign agents. This label, intended to delegitimize and stigmatize these entities promoting Western values or opposing the Kremlin's narratives, exploded in number after 2014. As reported by OVD Info, organizations labeled as foreign agents from 2015-2016 nearly quadrupled from the two years prior[1]. Consequently, this "law was instrumental in causing self-censorship and a mass exodus of domestic and international outlets from Russia, as well as forcing the remaining

[1] "Agents", *OVD Info,* available athttps://data-scripts.ovd.info/agents/

independent media organizations underground.[2]" By associating dissent with foreign interference, the Kremlin fostered anti-Western sentiment domestically. The West posed an existential threat to Russia's culture and geopolitical interests, thus creating a mentality that promoted nationalistic zeal among its citizens.

To further juxtapose the West from Russia, state media frequently framed the cultural morals underpinning Western influence as utterly irreconcilable with Russia's. Western nations were in a state of rapid moral decline, whereas Russia was a bastion of morality upholding traditional values. As part of Russia's response to defend against Western degeneracy, the military-patriotic program Yunarmiya was launched[3] to encourage patriotism among the youth, often depicting the West as an adversary undermining Russia's sovereignty. Following the 2022 Russian invasion of Ukraine, President Putin signed legislation decreeing the state's official traditional values and those entities that posed a threat to these values. These threats included: activities of extremist and terrorist organizations, individual media, actions of the United States and other unfriendly countries, and foreign NGO's.[4] By elevating traditional values to the level of state policy, Putin sought to unite Russian society around a nationalist and anti-Western ideology.

In conjunction with the expansion of the foreign agent law's power and the dissemination of state-sponsored information through media outlets, Russian state resources, including the

---

[2] Daniel Salaru, "Ten years of Russia's foreign agent law: Evolution of a press freedom crackdown", *International Press Institute,* "25 July 2022, available at https://ipi.media/ten-years-of-russias-foreign-agent-law-evolution-of-a-press-freedom-crackdown/

[3] "Military-patriotic movement "Yunarmiya" created in Russia", *Interfax,* 3 August 2016, available at https://www.interfax.ru/russia/521787

[4] "Putin approved the principles of state policy to strengthen traditional values", *Kommersat,* 9 November 2022, available at https://www.kommersant.ru/doc/5653496

Federal Security Service (FSB) and the Foreign Intelligence Service (SVR), actively identify and suppress critics of the government to promote nationalism. Well-known dissidents such as Alexei Navalny and Sergei Udaltsov have been the focus of FSB suppression campaigns. Interestingly, "the FSB is reviving the KGB tactic of the "prophylactic chat" meant to intimidate without the need for prosecution — or by interfering with the free flow of information. This involves measures including pressurising remaining independent media outlets such as Dozhd TV and using trolls to spam critical voices on the internet."[5] The proliferation of troll farms and bot networks has been a hallmark of Russian disinformation campaigns. They seek to amplify nationalist narratives and disrupt political stability domestically and abroad. Organizations like the Internet Research Agency (IRA), another state-backed entity, have systematically flooded social media platforms such as Facebook, Twitter, and Telegram with posts and comments that promote Kremlin ideologies and stir divisive sentiments in target audiences.[6] Through the use of automated bots and human staff, the illusion of widespread grassroots support for nationalist causes is quickly and persuasively created.

Internationally, troll farms have targeted Western audiences to exploit existing societal divisions and to sow distrust in democratic institutions. Following the 2016 Democratic National Committee (DNC) hack by groups attributed to Russia's SVR[7], IRA operatives used fake social media accounts to stoke political polarization and to push narratives misinterpreting and

---

[5] Mark Galeotti, "Putin's Hydra: Inside Russia's Intelligence Services", *European Council on Foreign Relations,* available at "https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf

[6] "Inside Russia's Notorious 'Internet Research Agency' Troll Farm", *Spyscape,* available at https://spyscape.com/article/inside-the-troll-factory-russias-internet-research-agency

[7] "Russia: UK and US expose global campaign of malign activity by Russian intelligence services", *Foreign, Commonwealth & Development Office,* 15 April 2021, available at https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services

exaggerating the contents of the leak. Additionally, the disinformation actors amplified content specific to the intended target audience to create as much havoc as possible. The Senate Intel Committee reports, "While the IRA exploited election-related content, the majority of its operations focused on exacerbating existing tensions on socially divisive issues, including race, immigration, and Second Amendment rights.[8]" The fallout from the exposed internal communications of the Democratic Party, causing the resignation of DNC leaders coupled with politically charged posts, proved to negatively shape American public perception of the 2016 election. Erosion of trust in the security election process and in the Democratic Party sowed discord among Americans and weakened democratic institutions with potential long-term implications for future elections. Both American public and digital infrastructure were inadequately prepared to respond to Russian disinformation campaigns crafted to destabilize U.S. democracy and align with the Kremlin's nationalist goal of weakening perceived adversaries. Consequently, the attack raised concerns about the security of U.S. political systems and the potential for foreign interference in future elections.

According to the Cybersecurity and Infrastructure Security Agency (CISA), "Disinformation actors use a variety of tactics and techniques to execute information operations and spread disinformation narratives that pose risk to critical infrastructure.[9]" These tactics include: cultivating fake or misleading personas and websites; devising or amplifying conspiracy theories; flooding the information environment; abusing alternative platforms; and spreading targeted content. Through carefully curated narratives disseminated by state media and online

[8] "Senate Intel Committee Releases Bipartisan Report on Russia's Use of Social Media", *Press Release of Intelligence Committee,* 08 October 2019, available at https://www.intelligence.senate.gov/press/senate-intel-committee-releases-bipartisan-report-russia%E2%80%99s-use-social-media

[9] "Tactics of Disinformation", *CISA,* available at https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf

platforms, the Kremlin has used disinformation to foster domestic unity, reinforce anti-Western sentiment, and position Russia as a counterweight against the decline of morals in the West. Accordingly, this has significantly shaped Western cyber strategies to address the unique challenges posed by Russian tactics. CISA has launched new cyber frameworks such as Protect 2020 and Shields Up as direct responses to the escalation in Russia's cyber activities. These frameworks provide guidance protecting voter databases, election equipment, and addressing disinformation campaigns targeting voters. Internationally, the European Union Action Plan Against Disinformation serves to detect disinformation campaigns after the Union "recognised the threat of online disinformation campaigns in 2015 when it asked the High Representative to address the disinformation campaigns by Russia.[10]" However, these campaigns are highly coordinated and state-backed, making them difficult to combat effectively without infringing on democratic values such as free speech. Automated detection tools powered by Artificial Intelligence (AI) are innovative solutions analyzing patterns in content dissemination, bot activity, and coordinated social media activity, yet the challenge of balancing security with the preservation of democratic principles persists. The decision-making algorithms of AI tools are notoriously proprietary and hidden[11], making it difficult to understand why certain content is flagged or removed. Political commentary, dissenting opinions, or satirical accounts that appear similar to disinformation campaign activity may be removed or shadowbanned, thus eliminating these accounts from legitimate public discourse. These concerns will become more relevant as AI technologically progresses.

---

[10] "Action Plan against Disinformation", *European Commission,* 12 May 2018, available at https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

[11]"What is AI transparency? A comprehensive guide", *Zendesk,* 18 January 2024, available at https://www.zendesk.com/blog/ai-transparency/

Within Russia, disinformation has been a powerful tool for unifying the population around a shared nationalist vision. Domestically, these campaigns foster unity by portraying Russia as defending against corrupt foreign influence and a bastion of moral strength. By positioning Russia as a moral alternative, disinformation campaigns resonate with domestic audiences who see their country as standing on the "right side" of history. This perspective significantly shapes their actions abroad pertaining to the West. Russia's cyber aggressions are justified as necessary responses to Western interference. Seen as a threat to the traditional values Russia holds dear, Western influence must be weakened. The rapid rise of these campaigns presenting significant challenges to Western democracies has become a catalyst for organized cyber governance and AI-powered detection tools. Democratic countries seeking to secure the integrity of their electoral processes with an informed populace must adapt to the threat of disinformation whilst striking a balance between security and the preservation of democratic principles.