



Russian Censorship

Treadstone 71



How censorship works in Russia.

Contents

Information War in Russia3

Pre-approved Information Sources3

Monitoring for Alternative Points of View.....4

Roskomnadzor.....4

SORM5

VEPR.....5

Laws in Russia.....6

Russian social media manipulators within the context of Russian censorship and
narrative control – an outline.7

Counteraction.....8

Audience Preparation9

Fostering National Pride and Confidence10

Projecting Superiority over Perceived Enemies11

Highlighting Domestic Achievements and Contrasting with Failures of Others11

Influencing International Perceptions11

Potential Risks and Challenges.....11

Closing.....11

The information war in Russia is not just the blocking of websites and the persecution of journalists. The system is much more complicated and built in such a way that the Russian media receive information on the topic of Ukraine, the European Union, NATO, and the United States, only from pre-approved sources. And specialized government agencies are constantly monitoring whether an alternative point of view has appeared in the media space.

Russia censors' information from getting to its citizens in a variety of ways, including:

- Blocking websites and social media platforms. Roskomnadzor, the Russian government's media regulator, maintains a blacklist of websites blocked in Russia. This blacklist includes websites that are critical of the government, as well as websites that are "extremist" or "terrorist." In recent years, Roskomnadzor has also blocked access to major social media platforms, such as Facebook, Twitter, and Instagram.
- Requiring media outlets to use only state-approved sources. In 2017, the Russian government passed a law that requires all media outlets to use only information from state-approved sources when reporting on certain topics, such as the military and elections. This law has made it much more difficult for independent media outlets to report on the news without fear of censorship.
- Using surveillance to track and punish dissent. The Russian government uses a variety of surveillance methods to track and punish dissent, including the use of SORM, a system that allows the government to monitor telecommunications traffic. This surveillance allows the government to identify and target people who are critical of the government or who are spreading "false information."
- Educating the public about the dangers of "fake news." The Russian government has launched a public campaign to educate its citizens about the dangers of "fake news." Russia uses the fake news campaign on fake news to justify the government's censorship efforts and to discourage people from seeking out information from sources that are critical of the government.

These are examples of how Russia censors' information from getting to its citizens. The Russian government's censorship efforts have been increasingly aggressive in recent years, and they have made it more difficult for Russians to access accurate information about the world around them.

Information War in Russia

1. **Beyond Blocking and Persecution:** While overt censorship methods like website blocking and jailing or fining journalists make headlines, subtle mechanisms are more pervasive. This includes exerting control over editorial policies, inducing self-censorship, manipulating algorithms to favor pro-government narratives, and more.
2. **State-controlled Media:** Major TV stations and newspapers controlled by the state, ensuring that the content aligns with the government's perspective. These media outlets play a key role in shaping public opinion.

Pre-approved Information Sources

3. **Filtered Narratives:** By ensuring that Russian media obtain their news from controlled sources, the state can ensure a consistent narrative across the country. This homogenization of news effectively narrows the range of permissible discourse.
4. **Ukraine, the EU, NATO, and the US:** These topics are of strategic importance to Russia. Given the illegal war in Ukraine, it is essential (from the state's point of view) that the narrative on these topics remains

controlled. For example, the annexation of Crimea in 2014 and subsequent portrayal of events in eastern Ukraine are very differently in Russian media compared to Western outlets.

Monitoring for Alternative Points of View

5. **Advanced Surveillance:** Russia has ramped up its surveillance capabilities, both technically and legislatively. Russian laws now require companies to store data of Russian citizens on servers within the country, making it easier for the government to access it. Similarly, the "Yarovaya Law" mandates telecom operators to store communication metadata for up to three years, used to track dissent.
6. **Crackdown on Oppositional Views:** Whenever an alternative point of view surfaces, there is a swift response, often under the guise of combating 'extremism' or 'foreign agents'. Russia uses these terms to target NGOs, opposition figures, or independent media.
7. **Forcing Self-censorship:** The consistent and arbitrary nature of these crackdowns induces fear, leading journalists, bloggers, and editors to censor themselves, avoiding topics that might land them in trouble.

The system in Russia is not just about shutting down voices; it is about controlling the narrative. This multifaceted approach – controlling media, filtering sources, and instilling fear – ensures that the government can maintain a grip on the information landscape.

However, like every other system, this one also has its vulnerabilities. With the advent of VPNs, satellite internet, and other technologies, Russians still find ways to access unfiltered information. The bigger challenge is making sure Russian citizens trust these alternate sources of information and that they resonate as much as the dominant narratives.

Roskomnadzor

Roskomnadzor, the Federal Service for Supervision of Communications, Information Technology and Mass Media, is a Russian government agency that is responsible for regulating the media and telecommunications in Russia. Russia uses Roskomnadzor as a tool of censorship to control the flow of information in Russia.

Roskomnadzor has tools used to censor information in Russia. These tools include:

- **Blocking websites:** Roskomnadzor can block websites that it deems to be illegal or harmful. This includes websites that contain pornography, child abuse material, or information considered to be a threat to national security.
- **Requiring websites to register:** Roskomnadzor can require websites to register with the agency. This gives Roskomnadzor the power to monitor and control the content of these websites.
- **Removing content from websites:** Roskomnadzor can remove content from websites that it deems to be illegal or harmful. This includes content that is critical of the government or that promotes dissent.
- **Fines and jail time:** Roskomnadzor can impose fines on individuals and organizations that violate its censorship rules. Roskomnadzor can even send people to jail for violating its censorship rules.

Roskomnadzor has used these tools to censor a wide range of information in Russia. This includes information about the war in Ukraine, the COVID-19 pandemic, and the Russian government's human rights abuses. Roskomnadzor has also censored information about opposition figures and independent media outlets.

The use of Roskomnadzor as a tool of censorship has had a significant impact on the flow of information in Russia. It has made it difficult for Russians to access information that is critical of the government or that promotes dissent. This has limited the ability of Russians to make informed decisions about their government and their lives.

The use of Roskomnadzor as a tool of censorship is a serious threat to freedom of expression in Russia. We must understand the ways in which Russia uses Roskomnadzor to censor information, and to take steps to protect your own freedom of expression.

SORM

SORM, or System for Operative-Investigatory Activities, is a system that allows the Russian government to monitor and collect data from telecommunications providers. This data includes phone calls, text messages, emails, and web browsing history.

The Russian government uses SORM to censor information. First, the government can use SORM to block access to websites that it deems to be illegal or harmful. This includes websites that contain pornography, child abuse material, or information considered to be a threat to national security.

Second, the government can use SORM to monitor the communications of individuals and organizations that it believes are a threat to the state. This allows the government to track the activities of these individuals and organizations and to identify potential threats.

Third, the government uses SORM to collect data to censor information after publishing. For example, the government can use SORM to collect data on the websites that Russians are visiting and the content that they are reading. Russia uses this data to block access to websites that contain information that the government does not want Russians to see.

The use of SORM to censor information is a serious threat to freedom of expression in Russia. It allows the government to monitor and control the flow of information in the country, and to silence dissenting voices. The use of SORM is also a violation of the right to privacy.

VEPR

VEPR, or the Virtual Electronic Public Review, is an automated system used by Roskomnadzor to censor information in Russia. VEPR identifies and blocks content deemed to be illegal or harmful by the Russian government.

VEPR works by crawling the internet and searching for content that matches a set of keywords or phrases. If VEPR finds content that matches a keyword or phrase, it will then analyze the content to determine if it is illegal or harmful. If VEPR determines that the content is illegal or harmful, it will block the content.

VEPR censors a wide range of information in Russia. This includes information about the war in Ukraine, the COVID-19 pandemic, and the Russian government's human rights abuses. VEPR has also censored information about opposition figures and independent media outlets.

The use of VEPR to censor information is a serious threat to freedom of expression in Russia. It makes it difficult for Russians to access information that is critical of the government or that promotes dissent. This has limited the ability of Russians to make informed decisions about their government and their lives.

Russia uses VEPR to censor information, controlling Russian citizen's freedom of expression.

Here are additional details about how VEPR works:

- VEPR is constantly crawling the internet, looking for new content that matches its keywords and phrases.
- VEPR uses a variety of algorithms to analyze content and determine if it is illegal or harmful.
- VEPR can block content on a variety of platforms, including websites, social media, and messaging apps.
- Roskomnadzor updates VEPR regularly with new keywords and phrases.
- VEPR is a powerful tool used to censor a wide range of information.

If you are concerned about your freedom of expression in Russia, it is important to be aware of VEPR and how it works. You can take steps to protect yourself from VEPR censorship, such as using a VPN or Tor. You can also contact your elected representatives and express your concerns about VEPR.

Laws in Russia

Censorship in Russia is a complex and ever-evolving system that uses a variety of methods to control the flow of information. The Russian government has laws and regulations used to censor information, including:

- Russia uses the Law on Countering Extremist Activity to ban websites and publications deemed to be extremist or terrorist.
- The Law on Information, Information Technologies, and the Protection of Information gives the government the power to block websites and censor information that it considers to be a threat to national security or public order.
- Russia uses the Law on the Protection of Children from Information Harmful to Their Health and Development to block websites and censor information that is harmful to children.

In addition to these laws, the Russian government also uses a variety of other methods to censor information, including:

- Direct censorship by government officials. This can involve ordering the removal of content from websites or publications, or even arresting journalists and bloggers who publish critical content.
- Self-censorship by media outlets and individuals. This is where people and organizations choose to censor themselves to avoid government scrutiny or punishment.
- Technical censorship. This involves using technical methods to block access to websites or censor content. Governments or private companies that are working on behalf of the government do this.

The level of censorship in Russia has increased significantly in recent years, especially since the start of the war in Ukraine. In March 2022, the Russian government passed a law that criminalizes the spread of "false information" about the war used to censor a wide range of information, including news reports, social media posts, and even artwork.

As a result of these censorship laws and practices, it is becoming increasingly difficult for Russians to access accurate and independent information. This is having a serious impact on freedom of expression and the right to information in Russia.

Russia translates news about Ukraine, but they change the translations pushing the Russian point of view, thereby controlling the narrative from seemingly foreign media sources. As a result, periodically, Russia media sources write about the decay of capitalism or LGBTQ indoctrination of children.

And only after that you can proceed to the development of counteraction scenarios. This is the answer to the question of how to neutralize the negative impact of the content.

Russian social media manipulators within the context of Russian censorship and narrative control – an outline.

State-sponsored actors or affiliated organizations use these tactics to shape public opinion.

1. Reaction to Opponents' Actions

1.1. Ensure Target Audience Does Not See Impact Content:

1.1.1. Organizational and Technical Measures:

1.1.1.1. Censorship:

- **Direct Intervention:** State authorities may directly intervene to censor content considered unsuitable. This can include direct removal of posts and videos.
- **Legislative Measures:** Russia enacts Laws to criminalize certain types of content or expressions.

1.1.1.2. Source Blocking:

- **Blocking Access to Specific Websites:** The government might block access to specific websites, channels, or social media platforms that promote opposing views.
- **Pressuring Platforms:** Governments may also pressure social media companies to take down or restrict access to certain content.

1.2. Make Target Audience Ignore Shock Content:

1.2.1. Divert Attention to a Brighter, More Interesting Event:

- **Promotion of Alternative Content:** Russia shifts attention away from critical or controversial issues by highlighting and promoting more appealing or sensational content.
- **Creation of Distractions:** Generating artificial controversies or events to keep the public engaged elsewhere.

2. Ensure Shock Content Does Not Affect Target Audience:

2.1. Form Distrust Among the Audience Towards Content, Author, or Source:

2.1.1. Refutation:

- **Counter-Narratives:** Creation of content that directly refutes shocking or undesirable content, using data, and testimonials.
- **Expert Opinions:** Using or mimicking respected authorities to debunk or refute the claims made in the content.

2.1.2. Discrediting the Source, Author, Content Delivery Channel:

- **Character Assassination:** Attacking the credibility of the author or source, often through personal attacks or highlighting past mistakes or biases.

- **Questioning Motives:** Suggesting ulterior motives or affiliations to devalue the content's credibility.

2.1.3. Ridicule and Bringing to the Point of Absurdity:

- **Satire and Parody:** Making fun of the content or exaggerating it to the point of absurdity to make it appear less serious or credible.
- **Memes and Viral Content:** Creating memes or humorous content that ridicules the original message.

2.2. Make the Content Unpleasant for This Target Audience:

- **Associating Negative Emotions:** Linking the content with something the target audience dislikes or fears, such as an unpopular political figure, group, or idea.
- **Utilizing Cultural Taboos:** Framing the content in such a way that it conflicts with widely held beliefs or cultural norms in the target audience.

The role of Russian social media manipulators in modern information warfare is complex. They not only remove or block content but also shape perceptions and steer public opinion in desired directions. The above strategies demonstrate the intricate nature of these operations, combining technical, psychological, and sociocultural methods. While governments and organizations use these tactics, within the context of Russia, they reflect the broader efforts to control and manipulate the information space.

Counteraction

Direct methods of counteraction, such as refutation, are often less effective in information warfare. We attribute this to factors such as the inclusion of psychological and cognitive aspects of how humans process information.

1. Audience Trusts Official Sources Less:

- **Credibility Gap:** Official sources have a vested interest or agenda, leading to skepticism.
- **Appeal of Alternative Narratives:** Russian social media trolls support alternative sources as more authentic or independent, thus perceived as more trustworthy.
- **Erosion of Trust in Institutions:** There has been a general decline in trust in governmental and official institutions. This can further drive audiences towards alternative sources.

2. First Impression Trap:

- **Priming Effect:** The first information received often sets the framework for understanding subsequent information. It is challenging to change this initial perception.
- **Confirmation Bias:** People tend to seek out and believe information that confirms their existing beliefs. If the first information aligns with their worldview, refuting it later may prove ineffective.

3. Emotional Neutrality of Rebuttal vs. Emotional Impact Content:

- **Emotional Engagement:** Impact content that appeals to emotions can be more persuasive and memorable. Emotions such as fear or anger can drive engagement and retention.
- **Analytical Rebuttals:** Refutations often come in a logical and analytical form, which may not engage an audience that has been emotionally stirred by the original content.

Strategies for Effective Counteraction:

Given these challenges, direct refutations can often be ineffective. Instead, Russian operators use a more nuanced approach:

- **Indirect Influence:** Rather than directly challenging misinformation, subtly guide the audience towards the desired conclusion. This can involve asking questions, fostering curiosity, and providing context that leads people to reassess their views.
- **Emotional Counter-Narratives:** Crafting counter-narratives that are equally emotionally engaging, using storytelling, imagery, and appeals to shared values or identity.
- **Utilizing Trusted Voices:** Using influencers, community leaders, or figures that the target audience trusts can bridge the credibility gap.
- **Long-Term Engagement:** Building trust and credibility with the audience over time, so when misinformation arises, the audience sees the counteracting source more credible.

The battlefield of information warfare is complex and requires a deep understanding of human psychology, communication dynamics, and cultural context. The limitations of direct refutation underline the need for multifaceted strategies that recognize and work with the inherent biases and emotional dynamics of the audience. In the context of Russia's information landscape, these insights are particularly relevant, given the often-polarized nature of political and social discourse. An effective strategy requires a combination of technological sophistication, psychological insight, and a keen understanding of the cultural and social fabric of the target audience.

Audience Preparation

Russian operators outline two key elements: preparing the audience for desired conclusions and a primary messaging injection.

1. Prepare the Audience for the Desired Conclusions:

1.1. Materials about Our Innovations:

- **1.1.1. Intensify the Dissemination of Materials on Modern Weapons:**
 - **Showcasing Technological Superiority:** By highlighting the supply and use of innovative military technology, the narrative fosters a sense of pride and confidence in national defense capabilities.
 - **Engaging Nationalistic Sentiments:** This tactic stirs patriotic feelings, thereby garnering support for governmental policies related to defense and foreign affairs.
- **1.1.2. Disperse Information from the Front Line About New Weapons:**
 - **Perceived Transparency:** This tactic gives the impression of a transparent and confident stance, showing readiness and cutting-edge capabilities.
 - **Reality-Based Narratives:** Using real-life examples and testimonials can make the narrative more tangible and credible to the audience.
- **1.1.3. Material About What and Where We Are Developing:**
 - **Showcasing Innovation:** Regularly updating the public on technological advancements helps keep an image of constant progress without compromising national security.

- **Engaging the Scientific Community:** This also promotes a positive image of collaboration between military, governmental, and academic institutions.

1.2. Materials about the Backlog of the Enemy:

- **1.2.1. Thesis about Outdated Western Weapons:**
 - **Undermining Confidence in Opponents:** Portraying Western weapons as outdated can reduce confidence in the capabilities of potential adversaries.
 - **Contrasting Strengths:** Russian operators create a favorable contrast by comparing the ineffectiveness of enemy weapons to domestic advancements.
- **1.2.2. Interest of NATO in Our New Models:**
 - **Creating an Aura of Envy:** This tactic helps frame Russian military technology as highly coveted and superior, even to technologically advanced Western nations.
 - **Intelligence Warfare:** Suggesting that other countries are trying (and failing) to get Russian technology for study can further the narrative of Russian superiority.
- **1.2.3. Failures of Western Development Programs:**
 - **Highlighting Competitors' Weaknesses:** Regularly discussing the failures of Western programs creates a narrative that contrasts sharply with the innovation and progress in domestic technology.
- **1.2.4. Publication with Hysteria from the Other Side:**
 - **Fostering Chaos and Desperation:** This tactic can amplify the perception of a chaotic and desperate enemy, further reinforcing the idea of Russian superiority and calm control.

2. Make the Main Modulating Injection:

2.1. About the Backlog of the West in the Development of Weapons:

- **Strategic Messaging:** This overarching message acts as the primary injection, synthesizing all the points from part 1 into a coherent narrative of Western decline and Russian ascent in military technology.
- **Long-term Psychological Impact:** By repeatedly asserting that the West cannot catch up with Russian advancements, this narrative can build a lasting perception of technological dominance, shaping public opinion and possibly even influencing international perceptions and policy decisions.

Russian narrative control is a complex and multifaceted strategy designed to shape public perception around current events and other key issues.

Fostering National Pride and Confidence

- **Unifying the Nation:** By emphasizing technological advancement and military strength, the narrative can foster a sense of shared pride and unity. In a diverse and complex nation, a strong and positive national narrative can be a powerful binding force.
- **Enhancing Government Legitimacy:** By projecting an image of strength and innovation, authorities can enhance their credibility and legitimacy in the eyes of the population.

Projecting Superiority over Perceived Enemies

- **Psychological Warfare:** The portrayal of superiority over perceived enemies serves not just a domestic purpose but can also play a role in psychological warfare, creating doubts and insecurities within rival nations.
- **Redefining Power Dynamics:** By emphasizing its technological and military superiority, Russia seeks to redefine power dynamics on the global stage, positioning itself as a leading power, particularly in contrast to Western nations.

Highlighting Domestic Achievements and Contrasting with Failures of Others

- **Selective Information Sharing:** The methodical crafting of these narratives involves selectively highlighting successes and innovations while minimizing or ignoring failures or setbacks. This paints a picture that might not be entirely reflective of reality but serves the purpose of shaping perceptions.
- **Creating a Dichotomy:** By juxtaposing domestic achievements with the failures of especially Western powers, Russia creates a dichotomy of "us versus them" that galvanizes public opinion and solidify national identity.

Influencing International Perceptions

- **Diplomatic Leverage:** By projecting an image of technological prowess, Russia can assert itself in international negotiations and garner more respect or fear from other nations. Russia uses this as a form of soft power to gain concessions in diplomatic discussions.
- **Geopolitical Positioning:** These narratives can be employed to realign geopolitical alliances and relationships. By asserting superiority over Western technology, Russia might attract nations interested in cooperation and partnership, especially in defense and technology sectors.

Potential Risks and Challenges

- **Credibility Gap:** If the narrative is too far removed from reality, or if it is perceived as mere propaganda, it might lead to a credibility gap, diminishing its effectiveness both domestically and internationally.
- **Strained Relations:** The aggressive portrayal of superiority and continuous undermining of Western powers may lead to strained diplomatic relations, impacting collaboration on global issues such as climate change, terrorism, or public health crises.

Closing

The strategies employed by Russia to shape narratives around military and technological superiority are multifaceted and have wide-reaching implications. While effective in fostering national pride and redefining power dynamics, they also present potential risks and challenges, particularly in international relations. Understanding these strategies is key for policymakers, diplomats, and analysts alike in navigating the complex web of information, perception, and power in today's global landscape. They illustrate how narrative control extends beyond mere domestic policy into the realms of diplomacy, psychology, and international strategy, reflecting the sophisticated interplay of communication in modern governance.

These issues include Russia's military prowess, technological innovation, and its role in the world. The government uses a variety of tactics to control the narrative, including:

- **Highlighting domestic achievements:** The Russian government often touts its successes in areas such as military spending, space exploration, and scientific research. Russia creates a sense of national pride and confidence in the government's policies through this narrative.
- **Contrasting with the failures of others:** The Russian government also frequently compares itself favorably to other countries, especially Western powers. Russia creates a sense of superiority and sows discord between Russia and its enemies.
- **Discrediting independent media:** The Russian government has cracked down on independent media outlets in recent years. This has made it more difficult for citizens to access information not controlled by the government.

The goal of Russian narrative control is to influence public opinion both domestically and internationally. By controlling the narrative, the government can shape how people think about Russia and its role in the world. This can have a significant impact on diplomatic relationships and geopolitical strategies.

In the context of the current war in Ukraine, Russian narrative control is playing a critical role. The government is using a variety of tactics to try to justify its invasion of Ukraine and to portray itself as the victim. This includes spreading disinformation about the war, suppressing independent media, and censoring social media.

The effectiveness of Russian narrative control is difficult to assess. However, Russia is investing heavily in this strategy. The goal is to create a world where everyone sees Russia as a powerful and legitimate actor, with unquestionable actions and motives.

www.treadstone71.com – We See What Others Cannot

www.cybershafarat.com