Strategic Comparative Intelligence Analysis (SCIA) Project

Disinformation Strategies: A Comparative Analysis of the United States and Russia

Kjersti Soberg

PS 505 – Comparative Intelligence Cultures

March 2, 2024

INTRODUCTION

In the contemporary digital landscape, disinformation has emerged as a formidable threat, undermining the integrity of democratic institutions and global security. Disinformation, defined as false information deliberately created and disseminated with the intent to deceive, mislead, or manipulate public opinion, stands in stark contrast to unintentionally spread misinformation. Its creation with the specific purpose of causing harm, influencing political processes, sowing discord, or undermining trust in institutions highlights its potency as a tool in information warfare. This paper focuses on the comparative analysis of the United States (US) and Russia, two nations with distinct political systems, media landscapes, and historical approaches to information control. It addresses the strategies employed by Russian, which prioritizes the instrumental use of disinformation for attaining strategic objectives, and the US, which emphasizes the development of countermeasures and defensive mechanisms to mitigate the harmful effects of disinformation campaigns. By examining the strategies of their intelligence communities to disinformation, this study aims to shed light on the broader implications for global security and the resilience of democratic institutions.

DISINFORMATION IN THE 21ST CENTURY: A GLOBAL CONCERN

Disinformation is a global concern, transcending national boundaries and impacting societies worldwide. The prevalence of these phenomena has been exacerbated by the advent of digital technologies, which have enabled the rapid spread and amplification of false information[1]. Countries and their policymakers are grappling with the challenge of combating this modern

[1] P.W. Singer and Emerson Brooking, *Like War: the Weaponization of Social Media*, 2019, 24.

challenge.[2] The interconnectedness of the digital landscape means that disinformation originating in one country can have far-reaching consequences, affecting global security and the stability of democratic institutions.

COMPARATIVE ANALYSIS OF STRATEGIES

While methodologies and platforms have evolved, disinformation campaigns are not a new phenomenon.[3] It is evident that the tactics employed by hostile foreign states have evolved from the Cold War era to the present day, yet their core objectives remain consistent: to undermine credibility, polarize society, and weaken democratic institutions. During the Cold War, the Soviet Union targeted the US with disinformation campaigns aimed at exploiting domestic tensions and spreading false narratives[4] Today, similar tactics are being employed by Russia, leveraging modern technology to disseminate disinformation more effectively and on a larger scale.[5] Disinformation is often seen as tools of state power, wielded to shape public opinion and advance national interests both domestically and internationally. The scale of these operations is significant, with state-sponsored media outlets playing key roles in disseminating false, government-aligned narratives.[6]

Beyond shaping public narratives, disinformation campaigns pose a significant threat to the core functions of intelligence agencies in both the US and Russia. In the US, the 2016 election serves as a stark example. Russia's sophisticated disinformation tactics, involving the

---

[2] Jon Bateman and Dean Jackson, "Countering Disinformation Effectively." Carnegie Endowment for International Peace, Washington, DC, 2024.
[3] Philip H. J. Davies and Kristian C. Gustafson, *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*, Washington, DC: Georgetown University Press, 2013, 97.
[4] Calder Walton, "What's Old Is New Again: Cold War Lessons for Countering Disinformation" Texas National Security Review, 2022.
[5] Ibid.
[6] U.S. Department of State, "Disarming Disinformation: Our Shared Responsibility." Press Release, 2024.

manipulation of social media platforms and human sources, aimed to sow discord and influence voter behavior.[7] This exposed vulnerabilities in traditional intelligence gathering methods, particularly the ability to discern credible information from fabricated narratives on social media. More recently, Russia's own intelligence services leverage disinformation as a weapon to manipulate the public and gain an edge in intelligence gathering. Its intelligence services fabricated narratives accusing Ukraine of harboring biological weapons were used to justify the 2022 invasion.[8] This highlights how disinformation can be weaponized to create a permissive environment for intelligence operations, blurring the lines between truth and fiction and manipulating information to advance Russia's strategic geopolitical objectives.

Russia's intelligence services have historically been well funded;[9] however, international sanctions and the war in Ukraine have placed strain on their budget.[10] This financial pressure could impact their ability to maintain their historical level of disinformation activities, offering a potential window of opportunity for the US to gain ground in combating this threat. In the US, countering disinformation competes with traditional intelligence priorities, demanding investments in specialized personnel, advanced detection tools, and public awareness campaigns.[11] This creates a trade-off, potentially hindering the effectiveness of traditional intelligence gathering activities as resources are diverted towards the ever-evolving threat of disinformation.

---

[7] United States, Senate Select Committee on Intelligence. "Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections." Volume 2: Report 116-XX, 2019, 3.
[8] Robert Lawless, "Ukraine Symposium – Russia's Allegations of U.S. Biological Warfare in Ukraine – Part I," Lieber Institute, West Point, 2022.
[9] Mark Galeotti, "Russian intelligence operations shifting tactics not goals," NATO Review, 2019.
[10] U.S. Department of the Treasury, "Treasury Sanctions Russian Intelligence Officers Supervising Election Influence Operations in the United States and Around the World," Press Release, 2023.
[11] The Heritage Foundation, "Russian Information Warfare: An Advancing Front of Disinformation and Propaganda," 2017.

SUCCESSES AND FAILURES

The fight against disinformation requires constant adaptation and learning. Examining successes and failures across different national contexts, including the US and Russia, allows us to address key questions: What other countries are concerned with disinformation and how are they tackling it? Are certain strategies more effective in specific environments? What challenges hinder global efforts? Given that disinformation is recognized as a serious threat globally, numerous countries have employed diverse strategies to combat it. In Southeast Asia, Malaysia, Singapore, and Thailand have successfully established fact-checking platforms that frequently publish corrections to avoid over propaganda.[12] Europe faces a major challenge from large-scale disinformation campaigns. The European Union (EU) has launched several initiatives and tools to tackle its spread and protect European values. These initiatives involve cooperation between EU institutions, online platforms, media, and citizens.[13] Russia is currently running a well-funded disinformation campaign in Latin America, targeting multiple countries with the aim of undermining support for Ukraine and promote anti-US/NATO sentiment.[14] While Latin America currently lacks robust laws against disinformation, some countries, like Brazil, are considering legislation.[15] Canada is also taking specific steps to counter Russian state-sponsored disinformation campaigns with a dedicated team, fact-based resources, sanctions, and international partnerships while upholding freedom of expression.[16]

---

[12] L. Schuldt, "Official Truths in a War on Fake News: Governmental Fact-Checking in Malaysia, Singapore, and Thailand," Journal of Current Southeast Asian Affairs, 40(2), 340-371, 2021.
[13] European Union, "Tackling online disinformation," European Commission, 2022.
[14] U.S. Department of State, "The Kremlin's Efforts to Covertly Spread Disinformation in Latin America," Media Note, 2023.
[15] André Duchiade, "New map sheds light on the state of disinformation legislation in Latin America and beyond," Knight Center, LatAm Journalism Review, 2023.
[16] Government of Canada, "Canada's efforts to counter disinformation - Russian invasion of Ukraine," 2024.

While efforts to combat disinformation have yielded positive results, a clearer picture emerges when also examining shortcomings and failures. Attributing disinformation campaigns remains a complex task, often hindered by the opacity of online operations and evolving tactics.[17] While initiatives like increased public awareness, fact-checking, international collaboration, and transparency efforts have shown promising results, challenges persist. For instance,

> Identifying disinformation presents several puzzles…labeling any claim as false requires invoking an authoritative truth. Yet the institutions and professions most capable of discerning the truth—such as science, journalism, and courts—are sometimes wrong and often distrusted. Moreover, true facts can be selectively assembled to create an overall narrative that is arguably misleading but not necessarily false in an objective sense.[18]

The US intelligence community has faced criticism for its failure to adequately anticipate and counter foreign disinformation campaigns, particularly those orchestrated by Russia. In some cases, the response has been reactive rather than proactive, allowing disinformation narratives to gain traction before being addressed. The decentralized nature of the US media landscape and the protection of free speech can make it difficult to regulate and control the spread of false information. The challenge is further compounded by the rapid evolution of digital platforms, which can quickly disseminate disinformation to vast audiences. As the US continues to refine its strategies, it must balance the need to protect national security with the preservation of democratic values and freedoms.

AREAS FOR NATIONAL AND INTERNATIONAL COOPERATION

The US Department of Homeland Security has undertaken several initiatives to combat

---

[17] Mercado, Stephen, "A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age," Central Intelligence Agency, Studies in Intelligence. Vol. 48. Issue 3, 2007, 45.
[18] Jon Bateman and Dean Jackson, "Countering Disinformation Effectively," Carnegie Endowment for International Peace, Washington, DC, 2024.

disinformation, primarily focused on election security and critical infrastructure. However, a department-wide strategy is lacking, leading to limitations and inconsistencies in their approach. While components like the Cybersecurity and Infrastructure Agency (CISA) and the Office of Intelligence and Analysis (I&A) have conducted threat analysis and issued public awareness materials, a lack of a unified vision restricts their effectiveness.[19] Limited authority due to privacy, free speech concerns, and the constantly evolving nature of disinformation tactics further complicate their endeavors.[20] Moreover, frequent leadership changes have hampered the development of a strategic focus on combating disinformation.[21]

Opportunities for global cooperation exist. For example, the Five Eyes alliance exemplifies successful information sharing and joint threat analysis.[22] Through secure communication channels and standardized protocols, they share intelligence on emerging disinformation campaigns, allowing for early detection and coordinated responses.[23] Collaborative fact-checking initiatives like the International Fact Checking Network promote cross-border knowledge sharing.[24] Standardizing regulations for online platforms and promoting responsible media practices can further strengthen collective efforts. While identifying a single best approach is difficult, learning from diverse strategies, enhancing digital literacy, and fostering international collaboration are crucial.

---

[19] U.S. Department of Homeland Security, "DHS Needs a Unified Strategy to Counter Disinformation Campaigns," Office of the Inspector General: OIG-22-58, 2022, 4.
[20] Ibid, 10-11.
[21] Ibid, 1.
[22] Frederic Lemieux, *Intelligence and State Surveillance in Modern Societies : An International Perspective*. Vol. First edition. Bingley, UK: Emerald Publishing Limited 2019, 61.
[23] United States, U.S. Senate Select Committee on Intelligence, Senate Report 117-2, 2021.
[24] RAND Corporation, "Fighting Disinformation Online," 2019.

BEST PRACTICES AND RECOMMENDATIONS

Advancements in technology, particularly in artificial intelligence (AI), present new avenues for manipulation. Deepfakes pose a significant threat, blurring the lines between reality and fiction.[25] The emergence of autonomous bots capable of spreading disinformation at scale further complicates the issue.[26] The rise of non-state actors with sophisticated capabilities and the potential for disinformation campaigns targeting critical infrastructure also introduce new dimensions of risk.[27] In *Enemies of Intelligence: Knowledge and Power in American National Security*, Richard Betts stated "to defeat outside enemies the main solution is to invest in more and better ways to penetrate their secrecy, unmask disinformation, and protect US assets through counterintelligence efforts."[28] Adapting strategies will require several key focus areas. Firstly, investing in AI-powered detection and analysis tools is crucial to identify and dismantle deepfakes and other AI-generated disinformation. Secondly, fostering international collaboration to share intelligence, develop common standards, and coordinate responses will be critical in countering the global reach of sophisticated disinformation campaigns. Thirdly, enhancing public education and media literacy is essential to equip citizens with the skills to critically evaluate information and resist manipulation. Finally, strengthening legal frameworks to address the misuse of technology and holding malicious actors accountable is vital to deter and disrupt their activities. By anticipating future trends and actively adapting their strategies, intelligence

---

[25] Robert Chesney, and Danielle Keats Citron, "21St Century-Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security, Maryland Law Review 78 (4): 882–91, 2019, 887.

[26] Himelein-Wachowiak M, Giorgi S, Devoto A, Rahman M, Ungar L, Schwartz HA, Epstein DH, Leggio L, Curtis B. Bots and Misinformation Spread on Social Media: Implications for COVID-19. J Med Internet Res. 2021 May 20;23(5):e26933

[27] Sarah Kreps Sarah and Richard Li, "Cascading chaos: Nonstate actors and AI on the battlefield." Brookings, 2022.

[28] Richard Betts, *Enemies of Intelligence: Knowledge and Power in American National Security,* New York: Columbia University Press, 2007, 10.

communities and countries can build resilience against the ever-evolving threat of disinformation.

CONCLUSION

Combating disinformation presents a formidable challenge, demanding not just individual solutions but collective action. While this paper has illuminated the contrasting approaches of the US and Russia, and underscored the potential of international cooperation, it is paramount to acknowledge the absence of a singular, definitive solution. Effectively countering disinformation requires a multi-pronged approach, encompassing proactive measures, robust international collaboration, and the empowerment of individuals. Its success hinges not only on individual efforts, but also on recognizing the inherent differences in intelligence cultures between nations like the US and Russia. These differences, whether rooted in historical approaches to information control, media landscapes, or political systems, influence the strategies employed and the perceived effectiveness of countermeasures. Ultimately, the fight against disinformation transcends national security concerns; it safeguards the very foundation of truth and trust upon which global stability and democratic institutions rely.

References

Bateman, Jon, and Dean Jackson. 2024. “Countering Disinformation Effectively.” Carnegie Endowment for International Peace, Washington, DC. https://carnegieendowment.org/files/Carnegie_Countering_Disinformation_Effectively.pdf.

Betts, Richard K. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security.* New York: Columbia University Press. https://search-ebscohost-com.ezproxy.bellevue.edu/login.aspx?direct=true&db=nlebk&AN=224617&site=eds-live.

Chesney, Robert, and Danielle Keats Citron. 2019. “21St Century-Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security.” Maryland Law Review 78 (4): 882–91. https://search-ebscohost-com.ezproxy.bellevue.edu/login.aspx?direct=true&db=a9h&AN=138261644&site=eds-live.

Davies, Philip H. J., and Kristian C. Gustafson. 2013. *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere.* Washington, DC: Georgetown University Press. https://search-ebscohost-com.ezproxy.bellevue.edu/login.aspx?direct=true&db=nlebk&AN=575822&site=eds-live.

Duchiade, André. 2023. “New map sheds light on the state of disinformation legislation in Latin America and beyond.” Knight Center, LatAm Journalism Review. https://latamjournalismreview.org/articles/new-map-sheds-light-on-the-state-of-disinformation-legislation-in-latin-america-and-beyond/.

European Union. 2022. “Tackling online disinformation.” European Commission. https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

Galeotti, Mark. 2019. “Russian intelligence operations shifting tactics not goals,” NATO Review. https://www.nato.int/docu/review/articles/2019/04/26/russian-intelligence-operations-shifting-tactics-not-goals/index.html.

Government of Canada. 2024. “Canada’s efforts to counter disinformation - Russian invasion of Ukraine.” https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng#a3.

The Heritage Foundation. 2017. “Russian Information Warfare: An Advancing Front of Disinformation and Propaganda.” https://www.heritage.org/europe/event/russian-information-warfare-advancing-front-disinformation-and-propaganda.

Himelein-Wachowiak M, Giorgi S, Devoto A, Rahman M, Ungar L, Schwartz HA, Epstein DH, Leggio L, Curtis B. Bots and Misinformation Spread on Social Media: Implications for COVID-19. J Med Internet Res. 2021 May 20;23(5):e26933. doi: 10.2196/26933. PMID: 33882014; PMCID: PMC8139392.

Johns Hopkins University. 2021. "Countering disinformation: improving the Alliance's digital resilience." NATO Review, Imperial College London & Georgia Institute of Technology. https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.

Kreps, Sarah, and Richard Li. 2022. "Cascading chaos: Nonstate actors and AI on the battlefield." Brookings. https://www.brookings.edu/articles/cascading-chaos-nonstate-actors-and-ai-on-the-battlefield/.

Lawless, Robert. 2022. "Ukraine Symposium – Russia's Allegations of U.S. Biological Warfare in Ukraine – Part I." Lieber Institute, West Point. https://lieber.westpoint.edu/russias-allegations-us-biological-warfare-ukraine-part-i/.

Lemieux, Frederic. 2019. Intelligence and State Surveillance in Modern Societies : An International Perspective. Vol. First edition. Bingley, UK: Emerald Publishing Limited. https://search-ebscohost-com.ezproxy.bellevue.edu/login.aspx?direct=true&db=nlebk&AN=1865289&site=eds-live.

Mercado, Stephen. 2004. "A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age." Central Intelligence Agency, Studies in Intelligence. Vol. 48. Issue 3. https://www.academia.edu/39908226/A_Venerable_Source_in_a_New_Era_Sailing_the_Sea_of_OSINT_in_the_Information_Age.

Office of the Director of National Intelligence. 2023. "Annual Threat Assessment of the U.S. Intelligence Community." https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

RAND Corporation. 2019 "Fighting Disinformation Online." https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html.

Schuldt, L. 2021. "Official Truths in a War on Fake News: Governmental Fact-Checking in Malaysia, Singapore, and Thailand." Journal of Current Southeast Asian Affairs, 40(2), 340-371. https://doi.org/10.1177/18681034211008908.

Singer, P. W., and Emerson T. Brooking. 2019. *Like War: The Weaponization of Social Media.* Boston: Mariner Books, Houghton Mifflin Harcourt.

U.S. Department of Homeland Security. 2022. "DHS Needs a Unified Strategy to Counter Disinformation Campaigns." Office of the Inspector General, OIG-22-58. https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-58-Aug22.pdf.

U.S. Department of State. 2024. "Disarming Disinformation: Our Shared Responsibility." Press

Release. https://www.state.gov/disarming-disinformation/.

U.S. Department of State. 2023. “The Kremlin’s Efforts to Covertly Spread Disinformation in Latin America.” Media Note. https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/.

U.S. Department of State. 2020. “GEC Special Report: Russia’s Pillars of Disinformation and Propaganda.” GEC Special Report. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

U.S. Department of the Treasury. 2023. “Treasury Sanctions Russian Intelligence Officers Supervising Election Influence Operations in the United States and Around the World.” Press Release. https://home.treasury.gov/news/press-releases/jy1572.

United States. 2021. U.S. Senate Select Committee on Intelligence. Senate Report 117-2. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

United States. 2019. Senate Select Committee on Intelligence. “Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections.” Volume 2: Report 116-XX. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Walton, Calder. 2022. “What’s Old Is New Again: Cold War Lessons for Countering Disinformation.” Texas National Security Review. https://tnsr.org/2022/09/whats-old-is-new-again-cold-war-lessons-for-countering-disinformation/.