

Russia's Strategic Messaging in Open-Source: How Propaganda, Censoring, and Dissidents  
Impacts their Current Message

Author - Joshua M. Carter

SOS 21C / Flight C34

April 02, 2021

Paper Advisor: Captain Daniel S. Kiser

**Disclaimer:** "Opinions, conclusions, and recommendations expressed or implied within are solely those of the author(s) and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other US government agency."

### **Abstract**

Russia's current message is one of re-achieving world power status by leveraging information, mainly through social media platforms, to propagate disinformation and exploit weaknesses of the United States and our Western allies. Moreover, Russia's capacity to do so has radically altered the battlespace, as witnessed by their involvement in the 2016 United States Presidential Election and the annexation of Crimea in 2014. In an era where access to information is widespread and cell phones have become a common household commodity, Russia's opportunities to further their influence in social media, misinformation, and propaganda broadcasting are ever-growing. To successfully disseminate a global message of the United States and Western weakness and relative Russian strength, Russia must engage in domestic censorship and quelling of dissidents that counter this intended message. For the United States and our Western allies to seek further success against Russia's virtual strength, we must apply a concerted effort towards public awareness of their actions and build corporate partnerships to combat and mitigate their capabilities.

## Introduction

Russia is fueled by a deeply rooted distrust of the United States and the West following the collapse of the Soviet Union, and this distrust influences how they operate strategically, operationally, and tactically in its competition with the West. Sarah Jacobs Gamberini, a Policy Fellow at the National Defense University, stated that "...Russia has had to be calculating and creative to balance its economic, military, and technological disadvantages to compete with the United States, maximizing less conventional tools of war, including covert operations within the information domain".<sup>1</sup> Moreover, their capacity to manipulate this information domain to influence its intended target's hearts and minds has radically altered this competition and the battlespace. Russia's current message is one of re-achieving world power status by leveraging information, mainly through social media platforms, to propagate disinformation and exploit weaknesses of the United States and our Western allies. The days of World War-esque face-to-face conflict conducted in trenches with enormous conventional forces are likely over, at least for the foreseeable future. Russia understands victory would be improbable given their current force disposition in a conventional conflict. These battles, unlike ever before, can now transcend a physical landscape towards a virtual environment with effects generated devoid of any conventional weaponry but rather a few keystrokes. Russia is highly proficient in this regard. John Heslen, a Ph.D. from Augusta University who specializes in cybersecurity, held that Russia is likely one of the most advanced global competitors concerning the cyber domain.<sup>2</sup> Consistent with this assessment, Russia invests in its virtual influence capabilities to elevate itself and weaken the United States and our allies in the West by creating further distrust and discord.

## Russia's Current Strategic Messaging

It is no longer as critical for Russia to amass surface-to-air missile systems, intercontinental ballistic missiles, or fifth and sixth-generation fighter aircraft like it was during the Cold War. They are aware of their limping economic status and capacity to mass-produce military inventory compared to the already present and growing inventory of the West,

---

<sup>1</sup> Gamberini, Sarah Jacobs. 2020. "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns." *Joint Force Quarterly* 5.

<sup>2</sup> Heslen, John. 2020. "Neurocognitive hacking: A new capability in cyber conflict?" *Politics and the Life Sciences* 94.

particularly the United States. These conventional means will remain relevant for Russian force posturing and regime defense. However, why expend large portions of their fiscal budget when they believe they can win a conflict in the open-source domain and avoid conventional warfare with the West altogether? T.S. Allen and A.J. Moore, both soldiers in the United States Army, argued that information has become a pivotal means of Russian power projection and can be used to compensate for their relative conventional weaknesses.<sup>3</sup> There are repeated examples of Russia's ability to use the information domain to generate propaganda aligned with their strategic intent of weakening the West's image on the world stage. This concept can be better understood by applying a case study methodology and analyzing Russia's involvement in the 2016 United States Presidential election.

Before the election, Russia initiated an overarching social media campaign whereby they employed "automated bots and paid trolls" to disseminate misinformation that sought to damage Hillary Clinton's campaign.<sup>4</sup> These bots and trolls aggressively constructed conspiracy theories. They pushed social media propaganda to the detriment of Hillary Clinton, all the while elevating Donald Trump's campaign, whom they believed would be a more advantageous candidate for the Kremlin. Several efforts within this campaign targeted the African American population to sway them from going to the polls and voting for the Democratic nominee.<sup>5</sup> Russia equates slavery and broader societal inequality as the "original American sin" and leveraged the crux of our strength, cultural diversity, as a means by which to diminish the American populace's faith in democracy.<sup>6</sup> It is challenging, admittedly, to ascertain the holistic impact this campaign had and whether it swayed voters' perceptions in a way that altered the results of the election. However, this activity did directly and effectively target and work to weaken the backbone of our democratic society.

---

<sup>3</sup> Moore, T.S. Allen and A.J. 2018. "Victory without Casualties: Russia's Information Operations." *21st Century Political Warfare* 59.

<sup>4</sup> Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, Elina Treyger. 2018. *Countering Russian Social Media Influence*. Santa Monica: RAND Corporation.

<sup>5</sup> Gamberini, "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns." *Joint Force Quarterly* 7.

<sup>6</sup> Frenkel, Scott Shane and Sheera. 2018. *The New York Times*. December 17. Accessed March 30, 2021. <https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html>.

## **Empowerment through Technology and Social Media**

Now consider the ever-evolving digital age and how social media was exploited in the case study. In an age where your cell phone, irrespective of brand, has more computing power than decades of previous technology combined, our regular connection to the internet and the growing prevalence of social media has never been greater. By accepting this interconnectedness and dependence on technology as reality, it is impossible not to acknowledge the potential this poses to Russia for furthering their propaganda output and social media targeting efforts against the United States and the West. Russia has fully embraced information and the open-source domain as a critical cog for propaganda and warfare. "Russia has used social media to foster conspiracy theories, plant rumors, and spread fake news in Bulgaria, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Serbia, Spain, Sweden, Ukraine, the United Kingdom, and the United States."<sup>7</sup> Russia's ability to cultivate schisms in democratic ideology is now more fiscally prudent and far-reaching than ever before as large portions of their intended target nations already have regular access to the internet and social media. They understand the virtual environment is difficult to defend against and the responsibility this puts on consumers of information to sift through false data to arrive at the truth independently. Defending against misinformation can be a laborious and challenging task that is often ignored or misunderstood, and they have become skilled at crafting elaborate conspiracy theories and fake news that is believable. Once misinformation has been considered and accepted, there is little chance of producing a "change of opinion," irrespective of how compelling the truth data challenging these conspiracies may be.<sup>8</sup>

## **Russia Managing the Message at Home**

Russia has established a comprehensive and wide-reaching censoring agenda to ensure the messaging their populace receives correlates with that of the Russian Federation's power and undertones of the West's weakness. In such a world, one could be constrained only to think in a way directed by Russia, the exact intent behind their censorship. Veronica Ma, a Staff Writer for

---

<sup>7</sup> Jakubowski, Glenda. 2019. "What's Not to Like? Social Media as Information Operations Force Multiplier." *Joint Force Quarterly* 9.

<sup>8</sup> Frank, Richard Stojar and Libor. 2018. "Information Dimension of the Contemporary Conflicts." *5th International Multidisciplinary Scientific Conference on Social Sciences and Arts* 110-111.

the Harvard International Review, explained that Russia makes considerable efforts to censor dissenting opinions of its population while using misinformation as an additional management measure. Their population receives the preponderance of their news and understanding of the broader world through Russian-controlled television broadcasts. As such, they can implement further restrictions towards the flow of information through this medium.<sup>9</sup> In line with the rest of the world, the introduction of social media and the open-source domain has complicated Russia's censorship effort. A polarizing example of how Russia responds to dissidence is witnessed by the events that captivated the world stage at the beginning of 2021 concerning Alexei Navalny.

Alexei Navalny, a man who stood in opposition of President Vladimir Putin, a proponent for political reforms, and an empowered voice to Russia's younger generations through social media, was covertly poisoned in an attempt to silence him. Alexei Navalny stood against the Russian federation, laying public siege to the communist regime and the corrupt nature in which they ruled. As a result, he was nearly killed and jailed immediately upon his return to Russia, having survived this poisoning effort.<sup>10</sup> As the news broke of his arrest, Russians took to the streets in a response that culminated in one of the largest widespread protests in the last decade. Russian police forces responded rapidly, disbanding the protestors they labeled as dissidents, at times resorting to brutality. Dissidence in Russia, underscored by this event, cannot stand as it serves to minimize censorship efforts and distract from their intended message of Western weakness by bringing to the world stage their own internal turmoil.

### **How History Can Help Predict the Future**

As Russia continues to improve its tradecraft in the open-source domain, its intent to weaken the United States and the West's influence and power is likely to reach outward throughout Eurasia. Sarah Jacobs Gamberini deduced that Russia has made active efforts to compete and lessen American power and global influence since the fall of the Soviet Union in 1991. Russia has applied a weight of effort on "asymmetric advantages" they believe they have over the United States and the West to compensate for their unequal conventional capabilities.<sup>11</sup>

---

<sup>9</sup> Ma, Veronica. 2016. "Propaganda and Censorship: Adapting to the Modern Age." *Harvard International Review* 49.

<sup>10</sup> Welss, Michael D. 2021. "Putin's Nemesis." *The View* 24.

<sup>11</sup> Gamberini, 5.

They have already demonstrated this perceived belief of Western weakness with the seizure of Crimea in 2014 and the Russian disinformation campaign that preceded and ensued throughout the incident. Before the physical annexation, Russia leveraged television broadcasts and manipulation in the open-source domain to disseminate pro-Russia propaganda to the Crimean populace as well as physically inserted Russian personnel into Crimea to spread further confusion. Exploiting the already present political turmoil within Ukraine, coupled with the chaos they created through television and online mediums that a large majority of the population ascribed to, they were able to accomplish the occupation without direct conflict or a defensive intrusion by Ukrainian forces. At the onset of the Crimea occupation, Vladimir Putin adamantly denied any Russian involvement on the world stage. However, he later admitted that Russian soldiers had, in fact, "seized Crimea."<sup>12</sup> By generating confusion within the open-source domain and a denial of involvement on the world stage, Russia was able to obtain control of Crimea with virtually no bloodshed while simultaneously subverting any Western intervention.

### **How Do We Win?**

In this digital awakening era, anyone with the correct means, often just a cellphone, can create and propagate information across large demographics. In this environment, Russia is currently thriving and operating nearly unhindered, pushing the United States and the West to develop mechanisms to mitigate their prowess rapidly. Luckily, we already understand their intentions and desire to re-achieve world power status by weakening the United States and our Western allies' influence. Knowing they are making efforts to exploit our weaknesses in the open-source domain and "defame America's reputation on the world stage," we must embrace a movement towards public awareness across all demographics to the volatility and scope of Russian virtual aggressions.<sup>13</sup> Doing so could render their impacts less meaningful and diminish their currently prevalent influence. Russia recognizes diversity as a key pillar within a democratic society, particularly for the United States, and recently used Twitter to flood data streams with content about the Black Lives Matter movement to "dilute legitimate related content." This social media campaign and any future open-source efforts will continue to be

---

<sup>12</sup> Moore, T.S. Allen and A.J. "Victory without Casualties: Russia's Information Operations." 63-64.

<sup>13</sup> Gamberini, 5.

leveraged to incite distrust and attempt to weaken Western democratic society because "US self-destruction would be Russia's ideal victory."<sup>14</sup> Awareness could force their hand in reimaging a strategy not as reliant on technology and capabilities in the virtual domain.

Additionally, our country must place a concerted economic and commercial effort towards developing our virtual mechanisms to mitigate and challenge Russia's actions. Our commercial sector, powered by corporations like Amazon and Google and influenced by social media platforms like Facebook, Twitter, and Instagram, must be postured and willing to support this initiative.<sup>15</sup> Without them, the United States and our Western allies stand little chance to mitigate the advancements Russia has already made and intends to make in the future. With the commercial sector's influence and the innovative prowess of our Airmen and broader allied military apparatus, we can stand against this fight and win.

---

<sup>14</sup> Gamberini, 7.

<sup>15</sup> Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, Elina Treyger. 2018. *Countering Russian Social Media Influence*. Santa Monica: RAND Corporation.



## Resources

- Chim, William. 2018. "Russia's Digital Awakening." *Connections: The Quarterly Journal* 5-16.
- Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, Elina Treyger. 2018. *Countering Russian Social Media Influence*. Santa Monica: RAND Corporation.
- Frank, Richard Stojar and Libor. 2018. "Information Dimension of the Contemporary Conflicts." 5th International Multidisciplinary Scientific Conference on Social Sciences and Arts 109-113.
- Frenkel, Scott Shane and Sheera. 2018. *The New York Times*. December 17. Accessed March 30, 2021. <https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html>.
- Gamberini, Sarah Jacobs. 2020. "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns." *Joint Force Quarterly* 4-11.
- Heslen, John. 2020. "Neurocognitive hacking: A new capability in cyber conflict?" *Politics and the Life Sciences* 87-97.
- Jakubowski, Glenda. 2019. "What's Not to Like? Social Media as Information Operations Force Multiplier." *Joint Force Quarterly* 8-16.
- Ma, Veronica. 2016. "Propaganda and Censorship: Adapting to the Modern Age." *Harvard International Review* 46-50.
- Moore, T.S. Allen and A.J. 2018. "Victory without Casualties: Russia's Information Operations." *21st Century Political Warfare* 59-70.
- Vasilescu, Alfred. 2011. "Evolution of Pathological Communication's Military Domains, From Propaganda to Information Operations." *International Conference of Scientific Paper AFASES* 275-283.
- Welss, Michael D. 2021. "Putin's Nemesis." *The View* 24.

