# Russian Disinformation Campaigns

"Information has become a destructive weapon just like a bayonet, bullet or projectile." – Vladimir Slipchenko, Russian military academic

## Introduction

The accessibility of online information has allowed Russian state and nonstate actors to parasitically inject misleading and false information with the intention of manipulating a target audience. **Disinformation** is false information that is deliberately created and intentionally spread with the intention of causing harm. Russia weaponizes disinformation to achieve a key strategic objective: the subversion of the West.[1] In the case of Russian Information Operations (IO), target audiences include the American population and the populations of other Russian adversaries.

When a democratic society no longer agrees upon a common set of facts, citizens begin to question firmly held truths and lose faith in their public institutions. Russian information operations administer damaging narratives against politicians, political parties, and/or hot-button issues like the COVID-19 vaccine into the American media space. By doing so, Russia  provokes the American electorate. Russia has material weakness relative to the United States, the Kremlin has managed to stave off its waning global influence through its superior use of information as a tool of "asymmetric statecraft."[2]

The dissemination of deceptive content online has proved to be more advantageous than engaging in conventional kinetic warfare: it is cost effective, can be executed without casualty, can be finely targeted and can be achieved clandestinely. Information operations operate in the gray zone "short of declared war" and allow Russia to engage in asymmetric warfare in which it can inflict damage on the United States by sowing social discord and political fragmentation.[3] Kremlin-based disinformation campaigns are carried out by Russian state and nonstate actors. Some are employed directly by Russian security services whereas others are carried out by non government entities such as the Internet Research Agency. Additionally, disinformation campaigns target states across the globe, not just the United States. These campaigns are not designed to change public opinion or convince a population of any one particular thing. They are meant to generate enough 'noise' in the online space to the point where societal divisions threaten the stability of a democracy ruled by a citizenry that no longer knows what is objectively true. In the words of a senior FBI official, "To put it simply, in this space, Russia wants to watch us tear ourselves apart."[4]

### The Goal of Russian Information Operations

[1] Allen, T.S., and A.J. Moore. "Victory without Casualties: Russia's Information Operations." *Parameters*, vol. 48, no. 1, spring 2018, pp. 59+. *Gale Academic OneFile*.

[2] Allen, T.S., and A.J. Moore. "Victory without Casualties: Russia's Information Operations." *Parameters*, vol. 48, no. 1, spring 2018, pp. 59+. *Gale Academic OneFile*.

[3] Allen, T.S., and A.J. Moore. "Victory without Casualties: Russia's Information Operations." *Parameters*, vol. 48, no. 1, spring 2018, pp. 59+. *Gale Academic OneFile*.

[4] Thompson, Terry L. "No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions." *Georgetown Journal of International Affairs*, vol. 21, no. 1, fall 2020, pp. 182+. *Gale Academic OneFile*.

The primary goal of Russian information-based warfare is to undermine the legitimacy of democratic governments by aggravating societal cleavages including racial, religious, political and ideological differences. By blurring the line between fact and fiction and intentionally fanning the flames of certain societal divisions, causes Americans to question their firmly held beliefs. This confusion and distrust across the U.S. population has threatened the stability of America's democratic institutions.

For Russia, employing informational and propagandistic campaigns is nothing new. During the height of the Cold War, Soviet "dezinformatsiya" campaigns were at the forefront of the Soviet Union's strategy for undermining and discrediting the United States. The Soviets funded communist newspaper outlets and radio stations that were broadcasted in the United States, along with publishing books written by authors paid by the Committee for State Security (also known as the KGB). KGB-funded publishing houses were even among the first to cast doubt on the Warren Commission's findings that Lee Harvey Oswald acted alone in the assassination of President Kennedy.[5] As technological capabilities have become more sophisticated in the digital age, so too have information warfare tactics used by Russia against the United States. Russia can no longer directly compete with Washington's military might and world influence, but it can cost-effectively influence America's democratic institutions by infusing distrust and confusion into the U.S. media space.

Russia can secure its strategic objectives against the West without having to invest in costly military operations or resort to physical force. The Kremlin can take advantage of the viral nature of internet platforms to exploit existing political fault lines and target specific subgroups of the American population with tailored messages that are designed to further polarize them. Steven Wilson, a political science professor at Brandeis University, eloquently describes the consequence of Russia's information warfare: "Democracy does not function without trust – in institutions, in the press, in fellow citizens. Russian disinformation campaigns have found social media a fertile field for destroying that trust."[6] If the information space becomes polluted with enough falsehoods, truth becomes relative. The goal is not to replace the truth with a single, individual lie – the goal is to sow doubt by making the "truth" an abstract concept.

**How Russia Injects Falsehoods**

In 2020, the U.S. Department of State characterized the Russian disinformation and propaganda ecosystem as having five key pillars: state-funded global messaging, cultivation of proxy sources, weaponization of social media, official government communications and cyber-enabled disinformation.[7] The first three pillars listed above are the central means by which Russian sows discord in the United States. *State-funded global messaging* includes campaigns mounted by Russian intelligence agencies like the FSB, a security service that succeeded the KGB, that spreads falsehood with the intention of undermining confidence in American leaders, institutions and further polarizing debates around hot-button issues. Russian intelligence agencies have targeted Western vaccines like Pfizer by publishing

[5] Giannetti, William. "A Duty to Warn: How to Help America Fight Back Against Russian Disinformation." *Air & Space Power Journal*, vol. 31, no. 3, fall 2017, pp. 95+. *Gale Academic OneFile*.

[6] Wilson, Steven. "What Are Russia's Goals with Disinformation on Social Media?" *BrandeisNOW*, Brandeis University, 22 Oct. 2020.

[7] https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

exaggerated reports of the risks that COVID-19 vaccines pose and their long-term side-effects. This fear-mongering taps into vaccine skeptics by exploiting deep-seeded anxieties over the safety of the vaccine and promotes the success of Russia's own vaccine, Sputnik V.

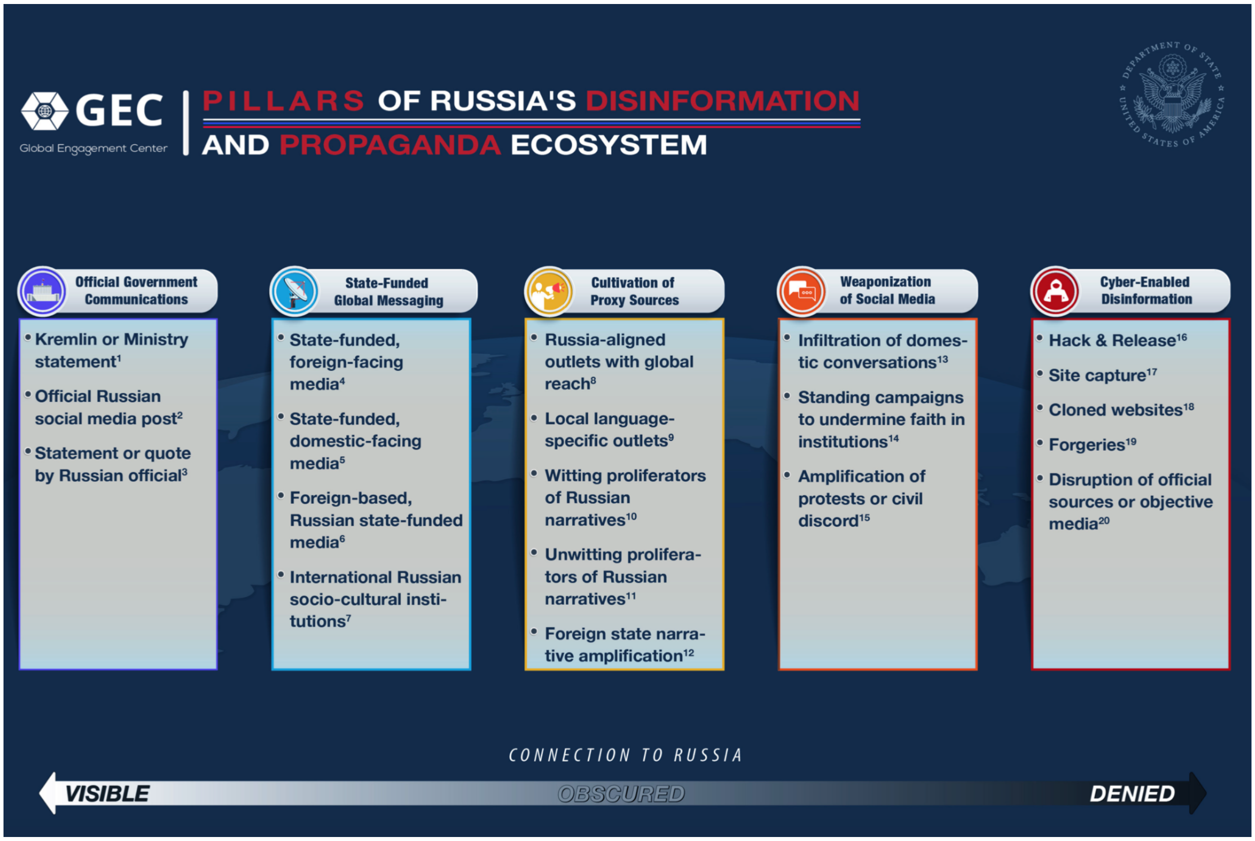
Another key element of Russian IO is the *cultivation of proxy sources*. Proxy sources are news outlets that are funded by the Kremlin, but attempt to maintain a veneer of separation to keep their connections to the Kremlin unclear, and thus dupe American readers into thinking that these sites publish independent work. They publish  the works of fringe Western thinkers and make the outlets appear to be based in the United States or Europe. Sources like *Global Research*, *The Strategic Culture Foundation, Geopolitica.ru, New Eastern Outlook* and *News Front* are all publications that are heavily immersed in Russia's disinformation ecosystem. *The Strategic Culture Foundation*, for example, is an online journal registered in Russia and directed by its Intelligence Service (SVR). These outlets publish conspiratorial content; recent examples include pieces blaming the U.S government for spreading COVID-19 or questioning Al-Qaeda's responsibility for the 9/11 hijackings.[8] According to the State Department's Global Engagement Center (GEC), *Global Research*, a conspiracy site operating out of Canada, received an estimated 12.370 million page visits between February 1 and April 30 of 2020. *The Strategic Culture Foundation* received nearly 1 million in the same period.[9] Russia's disinformation ecosystem is diverse and the lack of a central avenue of disinformation for their deceptive dissemination lets the information appear more credible and widespread.

Russia's *weaponization of social media* is also pervasive and cost-effective. It is important to note the connection between the business model underlying social media platforms and Russia's disinformation campaigns, as the two go hand-in-hand. The underlying economic logic of platforms like YouTube, Facebook, Instagram and Twitter is the monetization of user engagement. These large technology firms rely on data collection in order to create detailed behavioral profiles on individuals and their preferences, interests, likes, dislikes and beliefs. Sophisticated algorithms use this information to provide users with dynamically optimized stimuli and curated content. User data is sold to advertisers to create targeted advertising regimes that are tailored to each individual. By keeping users engaged, this business model has proved highly profitable.

However, nefarious actors like Russia can use this regime of targeted advertising, user data collection, and sophisticated algorithms to identify pockets of the voting population that are susceptible to false information.[10] Russian disinformation works on both sides of the aisle, inflaming both conservatives and liberal Americans. By using behavioral profiles of online users, Russian internet-agitators can find specific subgroups that share similar beliefs and target these groups with evocative social media posts or send them invitations to join Facebook groups centered on divisive topics like police brutality or immigration. For example, low-income populations were targeted with immigration and race-related advertisements, whereas middle-income populations were shown advertisements to join groups centered

[8] Joscelyn, Thomas. "How Effective Is Russia's Disinformation?" *FDD*, Foundation for Defense of Democracies, 6 Jan. 2021.
[9] https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf
[10] Ghosh, Dipayan. "It's all in the Business Model: The Internet's Economic Logic and the Instigation of Disininformation, Hate, and Discrimination." *Georgetown Journal of International Affairs*, vol. 21, no. 1, fall 2020, pp. 129+. *Gale Academic OneFile*.

around nationalism.[11] This demographic targeting stokes hyperpartisanship and furthers Russia's strategic objective to weaken.



GEC
Global Engagement Center

PILLARS OF RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM

**Official Government Communications**
- Kremlin or Ministry statement[1]
- Official Russian social media post[2]
- Statement or quote by Russian official[3]

**State-Funded Global Messaging**
- State-funded, foreign-facing media[4]
- State-funded, domestic-facing media[5]
- Foreign-based, Russian state-funded media[6]
- International Russian socio-cultural institutions[7]

**Cultivation of Proxy Sources**
- Russia-aligned outlets with global reach[8]
- Local language-specific outlets[9]
- Witting proliferators of Russian narratives[10]
- Unwitting proliferators of Russian narratives[11]
- Foreign state narrative amplification[12]

**Weaponization of Social Media**
- Infiltration of domestic conversations[13]
- Standing campaigns to undermine faith in institutions[14]
- Amplification of protests or civil discord[15]

**Cyber-Enabled Disinformation**
- Hack & Release[16]
- Site capture[17]
- Cloned websites[18]
- Forgeries[19]
- Disruption of official sources or objective media[20]

CONNECTION TO RUSSIA

VISIBLE — OBSCURED — DENIED

U.S. Department of State

Russian IO utilizes a variety of channels to manipulate American audiences via social media. The St. Petersburg-based Internet Research Agency (IRA), for example, is financed by allies of Putin and engaged in online influence operations by spreading conspiracy theories and incendiary messages to stoke discord on issues like race or religion in the run-up to the 2016 presidential election. The Kremlin-backed group, often called a "troll farm" – a professionalized group that coordinates the posting of provocative content using fake identities – employed an army of trolls to inject extreme content into the American media space and create an illusion of support for radical ideas.[12] Russian troll groups like the IRA bought and ran ads on Facebook and Instagram during the 2016 election, which according to MIT's *Tech Review*, "was reaching 140 million US users per month – 75% of whom had never followed any of the pages. They were seeing the content because Facebook's content-recommendation system had pushed it into their news feeds."[13] Social media algorithms tend to boost evocative and sensational information, and

[11] Alvarez, German, et. al. "Good News, Bad News: A Sentiment Analysis of the 2016 Election Russian Facebook Ads." *International Journal of communications* [online], May 2020, pp. 3027+. *Gale Academic OneFile*.

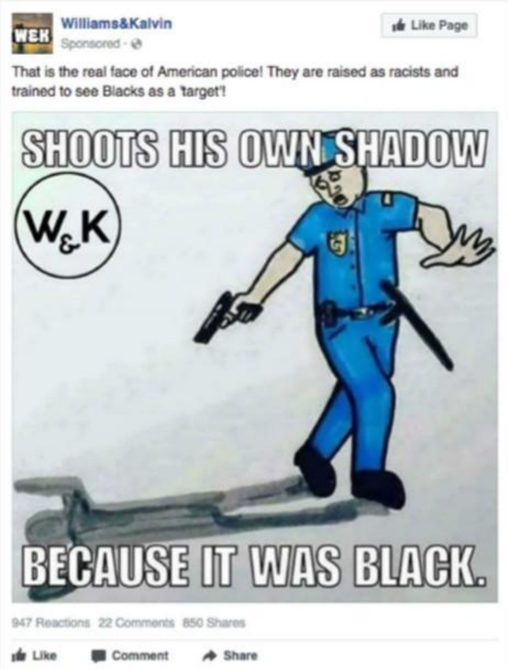
[12] Hao, Karen. "Troll Farms Reached 140 Million Americans a Month on Facebook before 2020 Election, Internal Report Shows." *MIT Technology Review*, MIT Technology Review, 20 Oct. 2021.

[13] Hao, Karen. "Troll Farms Reached 140 Million Americans a Month on Facebook before 2020 Election, Internal Report Shows." *MIT Technology Review*, MIT Technology Review, 20 Oct. 2021.

Kremlin-backed troll farms exploit this to proliferate disinformation in the American information space.[14] Troll farms and online bots pump out social media posts that are slogan-dependent, include heavy visuals and often utilize memes and humor.

**Known Russian Information Operation Example**

Up until 2017, a popular Facebook account called 'Blacktivist' used racial issues – particularly police brutality – to stoke outrage online. The account collected over 350,000 followers – surpassing the number of followers on the verified Black Lives Matter account at the time. Posts included videos of violent police arrests and messages such as "Black people should wake up as soon as possible."[15] In late 2017, it was discovered that Blacktivist was actually operated by Russia and designed to stoke racial tensions in the United States.



Williams&Kalvin

Sponsored ·

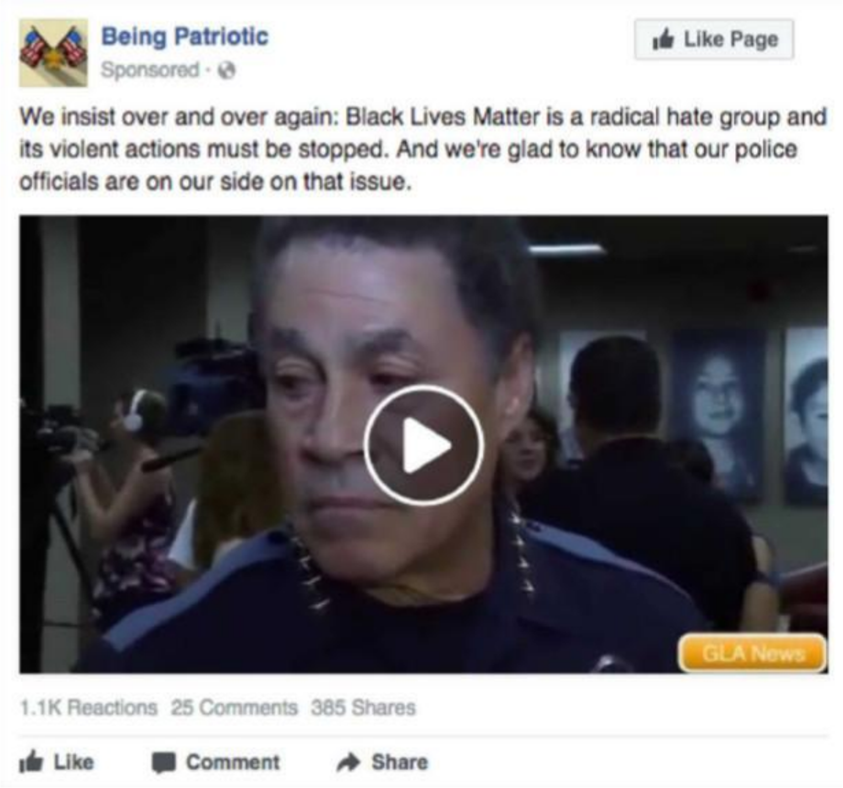
That is the real face of American police! They are raised as racists and trained to see Blacks as a 'target'!

947 Reactions 22 Comments 850 Shares

House Intelligence Committee, Facebook

[14] Alvarez, German, et. al. "Good News, Bad News: A Sentiment Analysis of the 2016 Election Russian Facebook Ads." *International Journal of communications* [online], May 2020, pp. 3027+. *Gale Academic OneFile*.

[15] Fung, Brian. "Russia Is the King of Disinformation on Facebook, the Company Says." *CNN*, Cable News Network, 26 May 2021.



We insist over and over again: Black Lives Matter is a radical hate group and its violent actions must be stopped. And we're glad to know that our police officials are on our side on that issue.

House Intelligence Committee, Facebook

**Preventative Measures and the Road Ahead**

Countering Russian information warfare is like a game of whack-a-mole: nobody knows when or where Russian disinformation will pop up, as it elusively resurfaces again and again. Online agitators can change their IP addresses and create new webs of bot accounts. Whereas Russian-sponsored posts were previously riddled with grammar and syntax errors that were specific to native Russian speakers – often omitting or misusing “a” or “the” because these indefinite articles are not used in the Russian language – Russian-sponsored posts have become more sophisticated in order to avoid detection.[16] Russian troll farms will now copy and paste chunks of text directly from other sources, use fewer hashtags and remove watermarks on images that had been previously taken down. Future disinformation campaigns may employ deep fakes – fake video and audio that appears convincingly real – that make it far easier to mislead audiences and create new suspicions about everything we watch. The possibilities for asymmetric information warfare are clear, but there are measures that can be taken to mitigate the impact of disinformation.

**Preventative Measures/Solutions**

[16] Alba, Davey. “How Russia's Troll Farm Is Changing Tactics before the Fall Election.” *The New York Times*, The New York Times, 29 Mar. 2020.

- **Artificial Intelligence (AI):** Emerging AI capabilities and machine learning may be able to discern and flag fake news on a large scale across multiple platforms.[17]
- **Education:** The American education system needs to emphasize digital literacy. Citizens need to be able to discern the truth by navigating and evaluating an increasingly muddled online information space. Researchers at Stanford University recently published a study revealing that more than 80 percent of students had a hard time discerning the credibility of the news they read. [18] A citizen capable of differentiating an ad from an article or real news from fake news will be less susceptible to disinformation.
- **Regulate Social Media Companies:** The United States comes far behind the EU when it comes to its regulatory apparatus for social media companies. The General Data Protection Regulation is a regulation in EU law that is designed to protect data privacy and apply pressure on big tech companies like Google and Facebook with fines for privacy violations. In terms of developing a minimally invasive method for monitoring social media content, the Czech Republic has come up with a sustainable model. There, a small unit of 15 social media analysts actively monitor platforms like Facebook, Twitter and other proxy sources that circulate disinformation.[19] The analysts simply flag the content as inauthentic – they don't censor or remove it. This type of content moderation respects America's veneration for freedom of the press and would not equate to content censorship.

## **<u>Sources:</u>**

Alba, Davey. "How Russia's Troll Farm Is Changing Tactics before the Fall Election." *The New York Times*, The New York Times, 29 Mar. 2020.

Allen, T.S., and A.J. Moore. "Victory without Casualties: Russia's Information Operations." *Parameters*, vol. 48, no. 1, spring 2018, pp. 59+. *Gale Academic OneFile*.

Alvarez, German, et. al. "Good News, Bad News: A Sentiment Analysis of the 2016 Election Russian Facebook Ads." *International Journal of communications* [online], May 2020, pp. 3027+. *Gale Academic OneFile*.

Domonoske, Camila. "Students Have 'Dismaying' Inability to Tell Fake News from Real, Study Finds." *NPR*, NPR, 23 Nov. 2016.

Fung, Brian. "Russia Is the King of Disinformation on Facebook, the Company Says." *CNN*, Cable News Network, 26 May 2021.

[17] McGeehan, Timothy P. "Countering Russian Disinformation." *Parameters*, vol. 48, no. 1, spring 2018, pp. 49+. *Gale Academic OneFile*.

[18] Domonoske, Camila. "Students Have 'Dismaying' Inability to Tell Fake News from Real, Study Finds." *NPR*, NPR, 23 Nov. 2016.

[19] Giannetti, William. "A Duty to Warn: How to Help America Fight Back Against Russian Disinformation." *Air & Space Power Journal*, vol. 31, no. 3, fall 2017, pp. 95+. *Gale Academic OneFile*.

Ghosh, Dipayan. “It’s all in the Business Model: The Internet’s Economic Logic and the Instigation of Disininformation, Hate, and Discrimination.” *Georgetown Journal of International Affairs*, vol. 21, no. 1, fall 2020, pp. 129+. *Gale Academic OneFile*.

Giannetti, William. “A Duty to Warn: How to Help America Fight Back Against Russian Disinformation.” *Air & Space Power Journal*, vol. 31, no. 3, fall 2017, pp. 95+. *Gale Academic OneFile*.

Gordon, Michael R., and Dustin Volz. “WSJ News Exclusive | Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines, U.S. Officials Say.” *The Wall Street Journal*, Dow Jones & Company, 7 Mar. 2021.

Joscelyn, Thomas. “How Effective Is Russia's Disinformation?” *FDD*, Foundation for Defense of Democracies, 6 Jan. 2021.

Hao, Karen. “Troll Farms Reached 140 Million Americans a Month on Facebook before 2020 Election, Internal Report Shows.” *MIT Technology Review*, MIT Technology Review, 20 Oct. 2021.

McGeehan, Timothy P. “Countering Russian Disinformation.” *Parameters*, vol. 48, no. 1, spring 2018, pp. 49+. *Gale Academic OneFile*.

Thompson, Terry L. “No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions.” *Georgetown Journal of International Affairs*, vol. 21, no. 1, fall 2020, pp. 182+. *Gale Academic OneFile*.

Wilson, Steven. “What Are Russia's Goals with Disinformation on Social Media?” *BrandeisNOW*, Brandeis University, 22 Oct. 2020.

U.S. Department of State GEC Special Report:

https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia’s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf