Putin's Information War Against the United States

Evans, Jacqueline

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Evans, J. (2022). Putin's Information War Against the United States. *Russian Analytical Digest*, 282, 9-12. https://doi.org/10.3929/ethz-b-000541999

ANALYSIS

Putin's Information War Against the United States

By Jacqueline Evans (George Washington University)

DOI: 10.3929/ethz-b-000541999

Abstract:
Information warfare between the United States and Russia is not a new phenomenon. However, recent developments, including an increase in Russia's disinformation activities, the social media revolution, and the invasion of Ukraine have created challenges for the United States, forcing officials to reevaluate current policies and develop new innovative strategies to combat the Kremlin's information warfare attacks.

A Strengthening Anti-American Campaign

Since taking power, Vladimir Putin has increased Russian efforts to weaken democratic institutions and Russia's perceived enemies via such informational warfare tactics as disinformation, propaganda, false flag attacks, and cyber-attacks. These measures, coupled with the widespread use of social media, have impacted numerous democratic nations. Yet recent interference in elections, including in the United States in 2016, and Russian-backed misinformation have highlighted gaps within American defense policy. As such, this article will examine the history of information warfare between the US and Russia, the threat posed and tools employed against the US, as well as the challenges and necessity of creating an all-encompassing response.

History of Information Warfare Between the United States and Russia

During the Cold War, both the US and the Soviet Union used covert disinformation tactics to challenge each other's ideological systems and gain influence around the world. Both nations spread conspiracy theories and rumors, distributed propaganda literature, set up front groups, carried out political operations, and engaged in election interference (Ward, Pierson, Beyer, 2019, p. 4–5). These tactics were not intended solely to target the domestic audience in the opposing country, but rather aimed at weakening alliances and partnerships to create division and make foreign nations question their relationship with either the US or the Soviet Union.

Information warfare concerned American officials so much that a working group, the Active Measure Working Group (AMWG), was created to combat Soviet misinformation by gathering information, analyzing reports, and then publicizing the evidence of interference and Soviet-created disinformation materials to educate the government and the public (Ward, Pierson, Beyer, 2019, p. 7).

There are some similarities between information warfare during the Cold War and today. With the rise of social media, however, the measures that worked in the 20th century are not necessarily effective any longer. The internet and social media have made it much more difficult to address disinformation because individuals can deliberately or inadvertently share conspiracy theories, propaganda, and fake news with thousands of people while circumventing traditional gatekeepers. Additionally, due to the openness of American society and the separation between government and businesses, the responsibility to monitor and remove misinformation posts lies with Big Tech rather than the government. The new ability of people to communicate among themselves rather than through traditional mass media and the power of platforms like Facebook, Twitter, and TikTok make the current environment very different from what existed previously.

Russia's Information Warfare Threat

Even though Russian information warfare is not a new concept, it still poses a massive risk to U.S. democracy and its ability to act on the international stage. To better understand the threat, it is important to understand why Russia is using informational warfare against the US, what Russia's goals are, and what the Kremlin is targeting.

All actions taken by the Kremlin are carried out to achieve Russia's geopolitical goals, including preserving its zone of influence in the countries of the former Soviet Union, attaining desirable opportunities to extend Russian sway internationally, expanding the Russian economy, and protecting Russian culture and society from information interference and psychological attacks (Gurganus and Rumer, 2019). To achieve many of these goals, Putin believes that Russia must undermine the standing of the US domestically, in Europe, and around the world, as the Kremlin sees the US as pursuing policies to maintain American hegemony and isolate Russia (Wojnowski, 2021).

At its core, Russia seeks to use information to exert psychological influence over individuals, societal groups, nations, and multilateral institutions (Saradzhyan, 2021). Therefore, Russia's information warfare targets U.S.

democracy to create internal divisions, increase political polarization, influence elections, and discredit democratic institutions, as well as strain relations between the US and its allies/partners through misinformation campaigns within and outside the US that exacerbate tensions and undermine coalitions (Wojnowski, 2021).

Essentially, Russia's goal in the US is to create so much polarization and division that Americans come to doubt the legitimacy of democracy and their government. Internationally, Russia hopes to weaken Western coalitions by promoting information that makes allies and partners question each other.

Tools Employed by Russia

To increase its impact, the Russian information warfare toolbox contains country-specific elements. Thus, the tools used against Poland, say, are going to be slightly different than the tools used against the US. The three main tools used against the US include the weaponization of social media, the use of proxy media sources, and cyber-attacks.

The Weaponization of Social Media: Arguably the most-used and best-known tool is the weaponization of social media platforms, including Facebook, Instagram, Twitter, and TikTok. This is achieved by amplifying division regarding protest or civil society disputes, supporting and contributing to disinformation campaigns that undermine faith in institutions and official government reports/information, as well as inflating domestic debates (U.S. Department of State, 2020 p. 8–9). Russia hopes that spreading misinformation and conspiracy theories on social media platforms will stoke division and polarization amongst Americans.

This is a serious issue, as an estimated 72% of Americans use some form of social media daily with about 53% obtaining news from social media (Pew Research Center, 2021; Shearer, 2021). Usage of social media combined with social media algorithms promotes personalized and popular content, meaning that Russia's weaponization of information has a chance of reaching and influencing millions of Americans (Meserole, 2018). Complicating matters further, users can share content not only on the original platform, but also on other platforms, making it difficult for companies to stop the spread of misinformation. Moreover, a study on misinformation and Twitter found that inaccurate information spreads faster and reaches more users than accurate information (Vosoughi, Roy, and Aral, 2018, p. 1147).

It is important to note that the weaponization of social media impacts not only American elections and politics, but also such societal issues as COVID-19 information, conversations about race, and immigration. The number of contentious issues within the US has allowed Russian operatives to both spread misinformation and amplify contention by posting controversial opinions that further divide Americans.

Proxy Media Sources: Russian operatives also use proxy media sources to extend their reach and make misinformation seem more credible. This tool entails spreading information through Russian-backed media outlets and Western media outlets knowingly or unknowingly reproducing Russian narratives.

Numerous Russian-backed media outlets operate in English and reach American audiences. Some of these sources, such as RT and Sputnik, are known Russian-backed media sites, while others are sites that average individuals may not realize have a connection with the Kremlin (U.S. Department of State, 2020). Websites including Strategic Culture Foundation, Global Research, New Eastern Outlook, and News Front are all Russian propaganda sites that operate in such a way that average users may not recognize the Kremlin connection (Joscelyn, 2020).

Aside from Russian-backed media outlets, there are also media platforms that knowingly and unknowingly spread Russian propaganda. This can occur in a couple of ways. First, a media outlet or journalist can knowingly spread information that is not fact-checked and promotes a pro-Russian narrative. For example, disinformation regarding COVID and the recent invasion of Ukraine that originates from Russia has been included in American news podcasts and news shows, including shows on Fox News (Brandt, Danaditya, and Wirtschafter, 2022). Although these individuals may not know that the information is false when they first report it, there are instances where they have continued to spread the information even after it has been debunked, thereby aiding in the spread of Russian misinformation.

News outlets can also inadvertently spread misinformation by giving air coverage to certain stories that aid Russia in weakening the relationship between nations. For example, according to a Polish expert, Russia frequently tries to divide Poland and the West by promoting claims that Poland is a far-right country (Polish Professor, 2022). Although it is important to highlight when the Polish government or other governments restrict civil liberties, it is also important that news outlets investigate the source of material and ensure that it does not inadvertently promote Russian talking-points.

Cyber-Attacks: Russia is notorious for using cyber-attacks and cyber-led efforts to create division and chaos within the US. Tactics include hacking and releasing hacked materials to disseminate damaging or sensitive information in order to make Americans question their government, institutions, or individuals (State Department, 2020). An example of this is the hacking of the Democratic National Committee (DNC) in 2016: Russian operatives hacked the DNC's computer server and

stole emails in the hope that it would damage presidential candidate Hillary Clinton's chances and thus help candidate Donald Trump (Director of National Intelligence, 2017). In the end, U.S. intelligence was able to determine that the cyber-attack had been carried out by Russia with a view to interfering in the election.

Together, these three tools have enabled Russia to successfully create and increase divisions between Americans. Additionally, the use of these tools makes it difficult for the US to attribute each effort to the Kremlin and Vladimir Putin, giving them some form of deniability.

The American Response

The increase in informational warfare efforts has not gone unnoticed by the US. Intelligence officials and members of the federal government recognize the risk these efforts pose to U.S. security. As such, these officials have scrambled to respond to the threat to protect democracy and the American way of life.

In 2016, under Executive Order 13721, President Obama created the Global Engagement Center (GEC) (Department of State Archive, 2001–2017). The GEC is housed in the State Department and was originally tasked with combating misinformation and messaging from ISIS (Department of State Archive, 2001–2017). However, the reach of the GEC expanded following the election interference conducted by Russia in 2016. Today, the GEC publishes reports outlining Russian information warfare tactics around the globe (U.S. Department of State, 2020). Most recently, as part of the effort to combat Kremlin misinformation regarding the invasion of Ukraine, the GEC and other offices of the State Department have started releasing Kremlin Disinformation Bulletins to document Russia's disinformation campaign in real time (United States Department of State, 2021).

Additionally, in 2018, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) created an inter-agency task force to counter Russian misinformation (Bodine-Baron, Helmus, Radin, and Treyger, 2018). This task force brought together DHS's Countering Foreign Influence Task Force and DOJ's Cyber Digital Task Force.

The intelligence community has also employed the tactic of revealing intelligence information regarding Russian information warfare campaigns as they occur to alert and warn both the public and private sectors. This occurred during the run-up to the 2020 election, when officials at the FBI and CIA warned that Russia was once again going to try and further polarize Americans and interfere in the election (National Intelligence Community, 2021). Additionally, the intelligence community and the Biden administration have in real time warned of misinformation efforts regarding COVID-19 and the invasion of Ukraine. Although such efforts are still relatively new, many pundits and experts believe they could be useful in beating Russia at its own game and helping to stop the spread of misinformation (Ott, 2021).

Outside the intelligence community and executive branch, Congress has begun to address this issue by holding hearings regarding the threat, considering legislation, and pressuring social media companies and executives to do more to stop their platforms from being used as Russian tools. Proposed legislation has ranged from sanctions against Russia to efforts to make political ads and social media data more transparent (Bodine-Baron, Helmus, Radin, and Treyger 2018). However, due to polarization within Congress, many legislative efforts have stalled.

Finally, under pressure from the government and the public at large, private companies have stepped up their efforts to combat Russian disinformation, including by increasing content monitoring, flagging false information, adjusting what political ads can be posted and by whom, and labeling political ads so users know that they are ads and may contain misleading information (Bodine-Baron, Helmus, Radin, and Treyger, 2018).

Most of these tactics have been implemented in the last 4–6 years, meaning the US is still severely behind in addressing the scope of Russian information warfare. In addition to the delayed response to threats, there are also challenges posed by the democratic essence of the U.S. political system.

Challenges and Gaps in the American Response

The biggest challenge facing the US is the need to respond while protecting the civil liberties and freedoms enshrined in the Constitution. First, under the U.S. Constitution, citizens have the right to free speech. Although there are some restrictions, overall, there are protected rights on social media to say how you feel and like or repost what you agree with. Free speech and freedom of expression are important facets of liberal democracies; efforts by the federal government to limit what people can say, like, or post on social media will be seen by many as censorship. This makes it difficult for the government to stop individuals and official media accounts from advertently and inadvertently spreading Russian misinformation.

Moreover, past intelligence community scandals that exposed spying and monitoring of American citizens and journalists have made the public wary of allowing the intelligence community to monitor and engage in fact-checking activities on social media and traditional media. Notably, a lot of the recent distrust of the government regarding its ability to fairly and accurately monitor content has been exacerbated by successful Russian information campaigns that have sought to polarize Americans.

Lastly, as evidenced by the debates regarding universal health care, business regulations, and pressure on social media companies, a key pillar of the American system is the separation between the government and the private sector. This principle carries over to the ability to address Russian information warfare because unlike other nations or even the EU, where there are more options for the government to regulate the private sector, in the US this is frequently debated and sometimes frowned upon. Together, this means that although the government can pressure social media and news outlets to be more proactive in addressing Russian propaganda and misinformation, there are limits to how much the U.S. government can force the private sector to act (Bodine-Baron, Helmus, Radin, and Treyger, 2018).

Although the lack of a coherent and strong response to Russian disinformation can be attributed to the need to respond effectively while protecting civil liberty, the harsh reality is that up until 2016, the US was not paying sufficient attention to the information warfare that Russia was conducting.

Conclusion

The threat of Russian information warfare and gaps in American policy responses highlight the dire need for a more sound and cohesive response. Without this, Russia will continue to use information warfare to sow chaos by dividing Americans and weakening democracy. Although these efforts are not new, they have been facilitated by the social media revolution, which has made information-planting and -sharing as easy as a click of a button, with the ability to reach millions of people in minutes.

Putin will not stop his assault on foreign democracy merely because he has been caught. Rather, he will continue to adapt and find new ways of disseminating misinformation. There are lessons to be learned and tools the US can adopt from other countries that have been dealing with this threat for over a decade. Yet it will take efforts by the federal government, the private sector, media outlets, and ordinary citizens alike to effectively and efficiently counter Russian information warfare.

About the Author

Jacqueline Evans is an M.A. candidate at George Washington University studying International Affairs with a focus on U.S. Foreign Policy and European/Eurasian Studies. She also holds a graduate certificate in International Security from the University of Arizona.

Bibliography:

- Brandt, J. Danaditya, A. and Wirtschafter, V. (2022). *Popular podcasters spread Russian disinformation about Ukraine biolabs*. Brookings. Available at: https://www.brookings.edu/techstream/popular-podcasters-spread-russian-disinformation-about-ukraine-biolabs/
- Bodine-Baron, E., Helmus, T., Radin, A. and Treyger, E. (2018). *Countering Russian Social Media Influence*. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf
- Department of State Archive. (2001–2017). *Global Engagement Center*. Available at: https://2009-2017.state.gov/r/gec/index.htm.
- Director of National Intelligence. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. DNI. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf
- Gurganus, J. and Rumer, E. (2019). *Russia's Global Ambitions in Perspective*. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/02/20/russia-s-global-ambitions-in-perspective-pub-78067.
- Joscelyn, T. (2020). *How Effective is Russia's Disinformation?* Foundation for Defense of Democracy. Available at: https://www.fdd.org/analysis/2020/08/12/how-effective-is-russias-disinformation/
- Meserole, C. (2018). *How misinformation spreads on social media—And what to do about it*. Brookings. Available at: https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it/
- National Intelligence Community. (2021). *Foreign Threats to the 2020 US Federal Elections*. National Intelligence Council. Available from https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf
- Ott, Haley (2021). *Information warfare expert says the U.S. is finally countering Russia at its own game*. CBSNews. Available at: https://www.cbsnews.com/news/ukraine-russia-information-warfare-disinformation-stopfake/
- Pew Research Center (2021). *Demographics of Social Media Users and Adoption in the United States*. Pew Research Center: Internet, Science & Tech. Available at: https://www.pewresearch.org/internet/fact-sheet/social-media/?menuItem=c14683cb-c4f4-41d0-a635-52c4eeae0245.