Fighting Disinformation
Countering Russian and Chinese Narratives Worldwide

Ebtisam Hussein (PhD, FU Berlin)
Associate Professor of Political Science, Cairo University
Associate Professor of Political Science, New Giza University
# Table of contents

1. Executive summery

2. Introduction

3. Defining Disinformation: what is it and why fight it?

4. Russia and China behind Disinformation Campaigns.

5. Global Efforts to Combat Disinformation

6. Any Way out for Democracies?

7. References
1. Executive Summary

In recent years, disinformation campaigns drew attention to the dangers associated with the vast proliferation of social media platforms, the enormous access to create and circulate content, and the potential use of such platforms in a new type of war between political antagonists. Disinformation is the deliberate spreading of false information, often aimed at inflicting harm on others. The US, the EU, NATO and the West at large are facing disinformation schemes at a global level, where both Russia and China are viewed as the key masterminds. Technology is central to both disinformation campaigns and global efforts to combat them. Both media literacy and coordination of efforts at state, regional and international levels are much needed to curb the disinformation tide but a key challenge remains for democracies to keep their citizens informed without restricting basic rights and freedoms amid fear of and protection against disinformation.

2. Introduction

The collapse of the former USSR gave hope that the cold war rivalry between the USA and the former USSR was over and that friendly relations between the USA and Russia were attainable. Yet, Putin’s presidency in 1999 instigated a twist in Russia’s foreign policy towards his country’s world status. His standpoints on the former USSR wrongful collapse, his aspirations to revive its glory, let alone financing pro-Russian and secessionist movements in Eastern Ukraine and unilateral annexation of Crimea in 2014 were all red flags indicating potential conflict and confrontation with the world’s superpower: the USA. Meanwhile, the economic rise of China was not accompanied by a direct political challenge to the latter. The Asian giant seemed initially focused on its economic growth and clear edge in international trade, with no substantial clues it was after open adversity with the USA. Yet, in 2018, a series of events indicated their relations might get rough: the USA-China trade war, then the COVID pandemic early in 2020 and most recently, and importantly, the Russian war in Ukraine. Initially, the war raised concerns on potential defiance of the USA superpower status (Gordon, 2022; Lynch, 2022) and was accompanied by overt gestures of cooperation between Russia and China. Simultaneously, both countries made strong claims against the West and the USA in particular, ranging from the presence of American biological weapons in Ukraine to the allegedly vicious role the USA plays to obstruct China from taking centre stage in the world. Expectedly, in today’s high-tech globalised world, trying to break the thrones of political rivals might take unconventional forms, especially if an open and direct war between major world powers is unlikely due to nuclear deterrence and/or symmetry in military capabilities. This policy paper seeks to highlight, in general terms, what disinformation is and why there is a dire need to fight it. It then, turns towards disinformation spread by China and Russia, global efforts to combat them and what could be done to counter them.

3. Defining Disinformation: what is it and why fight it?

Disinformation has a negative impact on people’s trust in the veracity of news and information they encounter in the public sphere. The public might, thus, question the value of free discussion and deliberation, especially when harassed online by disinformants when they express their opinions (Association of Progressive Communication, 2021). First, it is essential to highlight the difference between disinformation and misinformation. Disinformation deliberately spreads false and deceiving information which can lead to public harm. Misinformation is false or misleading content shared with no prior intention to harm, even if it ends up causing harm (Tackling Online Disinformation, n.d.). Other relevant terms include fabricated, manipulated, misleading and imposter content. Fabricated content refers to completely false content, while manipulated content means genuine information that has been distorted. Misleading content is different from both as it contains misleading information such as the presenting of comments or viewpoints as facts. Imposter content is also relevant to disinformation even if it is mainly about impersonating genuine sources not falsifying content (UNHCR, n.d.). Disinformation campaigns spread online using particular strategies, such as social engineering to provide a framework to manipulate events, inauthentic amplification using inauthentic accounts to promote false content or harass those with opposing views through the use of trolls and fake accounts (Feingold, 2022). Parties engaged in disinformation typically have political agendas and/or aims, be it electoral victories, promoting authoritarian settings, propagating populist policies, or inciting hatred against particular groups in society (Association of Progressive Communication, 2021, 6). This threat is global; virtually every country is a potential target of disinformation campaigns, with the culprits involving local, international, state and non-state actors (OECD, n.d.). Needless to say, social media furthers, even if unintentionally, the spread of disinformation campaigns. Often inauthentic accounts that masquerade as independent media outlets are created to post false content and have been developing their tactics to evade detection strategies deployed by social media platforms. Unsurprisingly, they make an effort to hide their tracks, for instance by using computer-generated photos to hinder detection through reverse photo searches. They also use handle switching, where they delete content when shifting to another operation. Content archiving is vital to spot these accounts. Some disinformation campaigns are even outsourced to third-party platforms (Goldstein &
Grossman, 2021). More profoundly, this problem is believed to spread not just because disinformation exists but also because of societal factors that promote its proliferation (Wilde, 2022). Several studies show that disinformation spreads much faster, or triggers more engagement, than true and accurate news on platforms like Facebook and Twitter (OECD, 2022). In addition, the Covid pandemic promoted anxiety and fear as it negatively affected job security, social relations and health. In such a context, disinformation spreads rapidly (Farinelli, 2021).

4. Russia and China behind Disinformation Campaigns.

In the last few years, there has been some controversy over the exact threat posed by Russia and China to the West asking which of the two constitutes a more imminent threat to security. While there is evidence that each poses different threats to the USA and its European partners, they increasingly align with one another (Scobell & Swanstroem, 2022; National Security Strategy, 2022 respectively). Today, as part of their rivalry with the West, Russian and Chinese spreading false information on the war in Ukraine are making headlines. Russia’s invasion of Ukraine on February 24th, 2022 (Askew, 2023) build on Putin’s denial of Ukraine’s status as a nation-state, claiming that it is part of Russia before the actual military aggression (Russia’s War in Ukraine, 2022). Furthermore, just a few weeks prior to the invasion, in December 2021, Russia steadily denied plans of military action against Ukraine, even when it was clearly increasing its artillery along its borders (Polito, 2021). Instead, Russia claimed it was preparing for military training, along with alleged threats to Russians in Ukraine in the parts of the country controlled by pro-Russian separatists since 2014 (OECD, 2022). In addition, it is trying to belittle the effectiveness of international sanctions, in an effort to undermine international pressure and condemnation of its 2022 war in Ukraine (Facts vs. Fiction, 2022).

Cross-cuttingly, five aspects are integral to the Russian disinformation campaign. These are: victimizing Russia as responding to hostility and Russophobia by others, denying historical facts to mislead the public on the righteousness of this war, promoting claims about the imminent collapse and demise of the West, portraying pro-reform popular movements as funded by the USA to foment political turmoil and intensively falsifying realities when the truth doesn’t work for its benefits/interests (Russia’s Top Five, 2022).

But Russia’s use of disinformation isn’t new as evinced by its notorious involvement in America’s 2016 presidential elections. Hillary Clinton’s campaign was hacked through a group of officers from an agency, the GRU, within the key Russian military intelligence directorate. This involved the hacking of email accounts of campaign staff and a few weeks later hacking both Democratic Congressional Campaign Committee and the Democratic National Committee (Beckwith, 2018). Russian efforts to manipulate these elections included setting up meetings with personnel working in the Trump campaign, stealing hundreds of thousands of voter information in a few states, leaking stolen emails and sharing them, through a fake online group named Guccifier 2.0, with WikiLeaks towards influencing election results (Abrams, 2019).

Likewise, during its war in Georgia 2008, Russia tried to justify its aggression by claiming ties with NATO and a prospect membership, thereby blaming Georgia for its military operation. Top political figures like Michael Gorbachev advanced the claim that Russia did not want to go to war (Fraser, 2022). Russia continued with disinformation schemes at the time of its 2014 annexation of Crimea, at the hope of garnering public support, claiming Ukraine provoked Russia into military operations against it. For instance, it accused Ukraine of committing atrocities against Russian-speaking people in the country’s east. Even worse, Russia claimed Ukraine would use weapons of mass destruction against civilians in Donbas and that NATO’s expansionism encircled Russia with enemies; thus, it was acting in self-defense (Delegation of the European Union, 2022). In 2014, disinformation campaigns used fake accounts pretending to be ordinary Ukrainian citizens to spread the idea that the protests that toppled back-then president Victor Yanukovych (who was pro-Russian) for his decision not to have closer ties with the EU, were actually a coup (Nakashima, 2017). In a similar vein, after annexing Crimea in 2014, Putin accused the West of interfering with the internal affairs of East European and Middle Eastern countries (Morrison, 2022).

Russian propaganda is reportedly rapid and repetitive but lacks consistency. It is produced in large volumes, using multiple channels. This multiplicity is effective, as receiving the same content from more than one source is more convincing, especially if different arguments with the same conclusion are presented through multiple sources (Paul & Mathews, 2016). An accurate depiction of Russian disinformation flooding social media platforms with false and misleading content is the following:

With Russian troll farms operating 24 hours a day, it is easy to see how these campaigns author new narratives and disseminate them widely and frequently. This approach essentially overwhelms the social media user with the amount of repetition and leads them to either accept the disinformation as fact or to fall back on their own baseline biases.

(Robbins, 2020)

As highlighted above, Russia’s deployment of disinformation was evident during earlier military aggressions, but this is not the case for the Asian economic giant. China has long invested in media influence but until recently no strong evidence was available that it was engaging in disinformation, comparable to that of Russia ahead of the 2016 elections in the USA (Cook, 2020). Today, it appears to actively be part of disinformation campaigns. While China’s bots and trolls on social media were already disseminating disinformation in 2019, their impact was regarded as modest. Two years later, various assessments of its disinformation efforts changed. More human and financial resources have been directed to these campaigns and Chinese disinformation efforts have become increasingly sophisticated and impactful. Its disinformation is remarkably persistent and adaptive; inauthentic accounts were taken down several times but they keep coming back. On Twitter, a network of fake accounts, linked to China,
was detected with its units almost separate from one another which made it more resilient (Cook, 2021). After the outbreak of the COVID-19 pandemic, China’s disinformation was strongly salient with its attempts to tell the world, as well as its own citizens, that the virus came from inside an American bio lab (Bachulska & Pu, 2020). It did not take the West much time to realise that both China and Russia were disinforming the world about the pandemic, as part of their rivalry to Western democracies:

As decision maker focus on shoring up their public health systems and economies, Russian and Chinese information campaigns are having a mutually reinforcing effect. Strong responses are needed from the United States, Europe, and democratic partners to ensure that authoritarian disinformation does not take root in fertile ground. (Brandt & Taussig, 2020)

One of China’s infamous disinformation strategies is the so-called Wolf Warrior diplomacy, referring to the remarkable increase in creating new, and strongly active, official accounts on social media platforms, representing Chinese diplomats and embassies. For instance, in March 2020, Zhao Lijian, from the Chinese foreign ministry shared articles on Twitter claiming the virus originated in the USA. The article was retweeted hundreds of thousands of times and cited in more than fifty languages (Twigg & Allen, 2021). Expectedly, China’s disinformation did not confine itself to the pandemic and in 2022, the FBI warned the headquarters of the Republican and Democratic parties that they could be targeted by hackers affiliated with the Chinese government (Sabin, 2022). According to Meta Platforms, a China-based Influence Operation targeted the 2022 elections in the USA, seeking to influence Meta users with political content. Luckily, the group was small and did not attract much of an audience; the operation was successfully disrupted (Paul, 2022). Even worse, as part of its attempt to delegitimize the USA, China alleges that there are American biological weapons in Ukraine and refuses to call Russian military actions against Ukraine an invasion (Bloomberg News, 2022). A key narrative taken over from Russian disinformation is that NATO is the aggressor, not Russia (FFC, 2022; Klug & Baig, 2023), as well as the distortion of the role of sanctions.

Last but surely not least, China is believed to amplify Russian disinformation. Based on statistical evidence, there was an increase in alignment on narratives propagated by Chinese and Russian officials; China gave preference to Russian standpoints on the war and Russian officials interacted at a higher rate with Chinese officials on online platforms. Their increasing online interaction, in the form of retweets, was clearly evident in the first third of 2022 and much of the content was anti-USA (FFC, 2022). China used state-run media, inter alia, to accuse Western media of inciting hatred against China. In fact, the deepening of Chinese-Russian relations is partly guided by their common narrative on the threats posed by alternative sources of information to their citizenry. Such claims are deployed by both countries in order to justify their crackdown on freedom of media and internet, calling for the “internationalization of internet governance” and they both agreed on the need to establish “cyber sovereignty” (Bandurski, 2022).

5. Global Efforts to Combat Disinformation

As much as technology has helped the spread of disinformation, it has also assisted in identifying it. Several techniques and softwares are currently employed to detect disinformation campaigns. Ad block Plus, Bot Sentinel, Botometer, Botslayer, Captain Fact, Disinformation Index, Media Bugs and Checkology are only some of the many tools that target content pertaining to disinformation (RAND, n.d.). Notably, efforts to combat disinformation are currently exerted at all levels: international organizations like the UN, regional entities like the EU, states like the USA as well as private enterprises such as Meta and Twitter are actively fighting disinformation.

The UN assigns high value to countering disinformation through its call to improve digital literacy and calls on states to hold accountable those who incite hatred of any kind, while warning against using defamation laws to curb freedoms (UN General Assembly, 2022). Similarly, the EU recently launched a platform to counter disinformation campaigns; the Information Sharing and Analysis Center will be in charge of tracking manipulation of information by non-EU countries. The EU is highly concerned with how these campaigns are organized to identify the culprits (Gouillard, 2023).

On its part, the United States is fiercely fighting disinformation by publicly countering its narratives. As stated earlier, ahead of the 2022 elections, Chinese disinformation was expected to target American politics and national security, the FBI Cybersecurity and Infrastructure Security Agency assured American citizens, that election officials took all necessary precautions to reduce the probability of malicious cyber activity that might jeopardize electoral infrastructure systems and/or data with the effect of altering, disrupting or preventing a vote cast (FBI & CISA, 2022). In addition, out of a realization that China is using social media in information warfare operations, and in anticipation of a potential conflict between the USA and China over Taiwan, experts warned that Chinese-American military personnel might be targeted by Chinese disinformation and recommended, inter alia, the USA should counter disinformation content on social media platforms (Harold et al, 2021).

Repeatedly, the USA fought disinformation through reporting on particular and detailed cases and filing charges against culprits in disinformation campaigns. For instance, it reported on Margarita Symonyan, a key Russian journalist and media figure with strong ties to the Kremlin, and her role in distorting information reported on the Beslan school terrorist attack in North Caucasus of 2004, receiving professional rewards in return. According to the American State department, Symonyan is just one of many disinformants associated with the Kremlin (Faces of Kremlin Propaganda, 2022).

Russia has long used disinformation as one of its most important weapons, creating a disinformation and propaganda ecosystem, in which the Russian intelligence is highly involved in (Disarming Disinformation, n.d.). This ecosystem is intended to raise doubts regarding
Gigantic social media platforms such as Meta and Twitter are based, by default, on allowing communication, debate and discussion. This is most likely the reason they boomed and attracted tens of millions of subscribers across the globe. To protect their community of subscribers and ensure the quality of their services, they seek, as pointed out earlier, to identify and takedown disinformation campaigns. Yet, their detection of trolls, fake accounts and such operations isn’t free of fault. As stated earlier, disinformants upgrade their strategies and tactics; this translates into both the possibility that some of disinformation goes undetected, at least for a while, and the persistent need to closely monitor and scrutinize the huge amount of content posted/shared/circulated on these platforms. After the attempts to manipulate the US 2016 elections, social media platforms took some tangible measures to spot disinformation; these comprised employing technology and hiring policy experts (Myers & Grant, 2023). Particularly, Social Media Influence Operations became an issue with Facebook and Twitter taking down tens of such operations between 2018-2020. In addition to the aforementioned China-based operation, another large and quite complicated one based in Russia was intercepted by Meta. The operation was a network of more than sixty websites mimicking real news organisations along with thousands of social media accounts and petitions. To augment its activities, it reportedly spent more than $100,000 on ads promoting pro-Russian messages and Russian embassies across continents amplified its content (Paul, 2022).

6. Any Way out for Democracies?
Realistically, rivalry through disinformation is likely here to stay. In a world, where weapons of mass destruction oblige rival countries to think twice, perhaps even thrice, before opting for open and direct military war, disinformation seems convenient to destabilise countries, justify wrongdoing and mislead the public. With the technological advances at human disposal today, countries like Russia and China can, with relative ease, exploit these means towards malign ends. Unfortunately, in several African and Asian countries, efforts to penalise disinformation led to restrictive rules and/or regulations that jeopardized basic rights and freedoms (Association of Progressive Communication, 2021, 15). In democracies, the core task of combating disinformation is multi-folded. Here’s a list of what it takes:

- Identifying disinformation campaigns and keeping up with their innovative ways of spreading their distorted content and on the other addressing the common tendency of not scrutinizing the sources of information we use to build our positions and share with others (Wilde, 2022).
- Democracies must deal with the strong flow of disinformation that was facilitated in recent years by the proliferation of social media platforms. They must educate their citizens about disinformation, its strategies and dangers. This requires orchestrated efforts involving both government and non-government sectors investing in media literacy.
- Specific skills are quite helpful in this respect; these include identifying details in any text, what it says and how it is said, if there are any patterns, similarities or contradictions, etc. (Kain, 1998) and realizing how different media types (TV, radio, websites, etc) can affect the way a message is delivered (Bordac, 2009) and how media outlet ownership can impact its content.
- Democracies shouldn’t turn into autocracies by sacrificing democratic ideals and institutional arrangements through setting limits on free access to information as a means to protect the populace from its vices. Combating disinformation does not entail infringing on basic rights and freedoms.
- Instead, democracies must secure access to reliable sources of information to help the masses learn about domestic and international politics away from both disinformation and misinformation.
- Technological advances are central to fighting disinformation and thus countries with an edge in digital-technology industries could develop better protections against disinformation.
- Finally, coordination across various levels is strongly recommended: international, regional, state as well as private enterprises should join efforts. This entails developing relevant structures and mechanisms for this coordination to take place.
7. References


- ——— (2021), Beijing is Getting Better at Disinformation on Global Social Media, *The Diplomat*, March 30, at: https://thediplomat.com/2021/03/beijing-is-getting-better-at-disinformation-on-global-social-media/

- Delegation of the European Union to the People’s Republic of China (2022), Disinformation about Russia’s Invasion of Ukraine-Debunking Seven Myths Spread by Russia, March 18, at: https://www.eeas.europa.eu/delegations/china/disinformation-about-russias-invasion-ukraine-debunking-seven-myths-spread-russia_en?;s=166

- Department of Justice (2018), Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election, Office of Public Affairs, July 13, at: https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

- Disarming Disinformation: Our Shared Responsibility (n.d.), *State Gov*, at: https://www.state.gov/disarming-disinformation/


- Feingold, Spencer (2022), The Four Key Ways Disinformation Spread Online, *World Economic Forum*, Aug. 9, at: https://www.weforum.org/agenda/2022/08/four-ways-disinformation-campaigns-are-propagated-online/


- Fraser, C (2022), How Russian Disinformation Tactics were Utilised in the Context of 2008 5day War, *Institute for Development of Freedom of Information*, Nov. 3, at: https://idfi.ge/en/how_russian_disinformation_tactics_were_utilised_in_the_context_of_the_2008_5_day_war


- Kain, P. (1998), How to do a Close Reading, for *The Writing Center at Harvard University*, at: https://writingcenter.fas.harvard.edu/pages/how-do-close-reading


--- (2022), Disinformation and Russia’s War of Agression against Ukraine: Threats and Governance Responses, Nov. 3, at: https://www.oecd-ilibrary.org/docserver/37186bde-en.pdf?expires=1676839999&id=id&accname=guest&checksum=70C403A5A04AA82E89B6EAA33EDBB065


-Politico (2021), Kremlin Denies Plans to Invade Ukraine, Alleges NATO Threats, Dec. 11, at: https://archive.ph/GpG6p


-Russia’s Top Five Persistent Disinformation Narratives (2022), State Gov, Jan. 20, at: https://www.state.gov/russias-top-five-persistent-disinformation-narratives/

-Russia’s War in Ukraine: Six Months of Lies, Implemented (2022), State Gov, Aug. 24, at: https://www.state.gov/disarming-disinformation/russias-war-on-ukraine-six-months-of-lies-implemented/


