PEPPERDINE UNIVERSITY

Global Tides

Volume 17 Article 8

April 2023

A Fake Future: The Threat of Foreign Disinformation on the U.S. and its Allies

Brandon M. Rubsamen
Pepperdine University, brandon.rubsamen@pepperdine.edu

Introduction

Take a look at these recent news headlines: "*Anger grows in S. Korea over US-run labs*," "*Military personnel of Ukrainian Armed Forces launched a missile strike on a peaceful civil enterprise*," and "*President Zelensky surrenders to Russia, 'it didn't work out…'*."[1] What does each of these captions have in common? Anyone guessing that they were all fake or government-run propaganda would be correct. These article titles come from China Daily (owned by the Publicity Department of the Chinese Communist Party), the Russian Ministry of Defense, and Ukraine-24, respectively.[2] All of these posts, in one form or another, are misinformation. Specifically, they are all campaigns of malign disinformation. Disinformation campaigns by Russia, China, and other actors pose a significant risk to U.S. intelligence operations and national security. The United States and its allies must take action against all forms of misinformation before malign actors realize its maximum effect.

The History of Disinformation

Misinformation is any form of false or inaccurate information, primarily when found on open-source platforms or in the media. Disinformation takes this definition one step further by applying harmful intent to the dissemination of misinformation – usually by governments or malign actors. Because some misinformation, like the articles listed above, is easily identified and refuted, it may seem that disinformation campaigns pose only a minor threat to U.S. national security and the general public. However, attacks like the Ukraine-24 hack display disinformation's propensity to endanger public opinion and infect historically trustworthy institutions. The 2016 and 2020 U.S. presidential elections have also been cited as cases in which Russian propaganda influenced voter behavior and drove party polarization. The effects of these examples and others like them create an environment in which civilians and governments do not know what to trust. As awareness about the harms of disinformation campaigns grows, so do such campaigns evolve in complexity – and at an alarming rate. As the above headlines demonstrate, malign disinformation targets not only Americans but also their allies abroad.

Despite the recent focus on weaponized disinformation in the Ukraine conflict and the 2016 U.S. presidential elections, Russian disinformation operations are nothing new. The roots of strategic interference can be traced back to the 1980s with *Operation Denver*,[3] a Soviet campaign to convince the world that the United States had created the AIDS virus. It took the State Department six years to debunk the campaign and prove Soviet involvement, but even then, "there are millions of Americans who still believe in that hoax today" (Schifrin and Ellick). Since the 1980s, the U.S. government, media outlets, and the American public have become more proficient

[1] See https://tinyurl.com/ChinaDaily-disinfo, https://tinyurl.com/RU-DefMin-Facebook and, https://tinyurl.com/Zelensky-deepfake, respectively, for the disinformation examples. It seems inappropriate to actually give credit to these sources, which is why they are provided here, rather than in the bibliography.

[2] The lattermost article, found on a Ukrainian news website, resulted from a foreign hack and has since been taken down.

[3] Popularly but incorrectly known as *Operation Infektion*

at discerning fake news. However, malign actors have counteracted this increased proficiency by becoming more adept at producing and disseminating disinformation. Whereas Operation Denver was a singular, carefully planned, and executed attack, Russian propaganda today is a "firehose of falsehood," in which disinformation is broadcast in high volume across various mediums and channels (Paul and Matthews). Virtually any online platform in any country – ally or rival – is at risk.

The Risk of Disinformation

Since the Cold War, Russia has held the monopoly on disinformation, being the only country to employ it pervasively and consistently on an international scale.[4] Realizing the efficacy of such malign campaigns, China recently began emulating its northern neighbor with new operations of its own. The Office of the Director of National Intelligence (DNI) cites the risks of Chinese misinformation and Russian disinformation to U.S. influence in its 2022 Annual Threat Assessment.[5] In addition to spreading misinformation regarding COVID-19, China will continue learning from Russia's model of disinformation and begin "intensifying efforts to mold U.S. public discourse" (DNI). The same report lists the ongoing threat that Russian propaganda holds for its rivals and especially in U.S. elections and political polarization.[6]

The Eurasia Group also lists Russian disinformation as a top future risk – concurring with the U.S. Intelligence Community (IC). They forecast more election interference ahead of the 2022 midterms and the 2024 presidential election in order to build distrust and "sow greater discord in a deeply divided superpower" (Bremmer and Kupchan). Even more worrisome is Eurasia Group's prediction that Russian intelligence will take a more direct role in the spread of disinformation and even the hacking of U.S. officials. Until now, Russian hacking and propaganda have primarily been performed by proxies of the government, which rarely directly attack foreign governments or combine disinformation with cyberattacks. Eurasia Group's suggestion would be a bold and

[4] While China has often used misinformation campaigns and censorship domestically and against Taiwan and Hong Kong, until recently it has refrained against levying such strategies against the U.S., it allies and partners (Harold et al., 2021). Recently, the CPP has disseminated COVID-19 misinformation globally and begun joint operations with Russia against the West in 2022 (Bandurski). An example of a joint disinformation campaign is China spreading false Russian claims that the U.S. is housing biological weapons in Ukraine (Bandurski, Price).

[5] The DNI's report is wary that "China will continue spreading COVID-19 misinformation and downplaying its early failures while casting blame on the West. Its misinformation includes claims that the United States created COVID-19" (8). Furthermore, in respect to Russia, the DNI reports, "Moscow almost certainly views U.S. elections as opportunities for malign influence as part of its larger foreign policy strategy. Moscow has conducted influence operations against U.S. elections for decades, including as recently as the 2020 presidential election. We assess that it probably will try to strengthen ties to U.S. persons in the media and politics in hopes of developing vectors for future influence operations. Moscow almost certainly will continue these online influence operations in the United States and in countries such as Belarus, Ukraine, and other countries of key Russian interest. Moscow will also continue and seek out new methods of circumventing technology companies' anti- disinformation activities to further expand its narratives globally" (12).

[6] In its report, the DNI warns "Russia presents one of the most serious foreign influence threats to the United States, using its intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances, and increase its sway around the world, while attempting to undermine U.S. global standing, amplify discord inside the United States, and influence U.S. voters and decision making." (12).

dangerous step in the evolution of Russian information warfare – showing just how frayed Western relations have become with Russia and how weak Russia perceives the former's defenses to be.

The War in Ukraine and Other Pressing Issues

Developments since the DNI and Eurasia Group's early 2022 reports indicate the reality of this disinformation evolution and the threat it poses. However, what reports failed to predict was the exacerbating effect that Russia's invasion of Ukraine would have on misinformation campaigns. One needs to look no further than the Twitter or Facebook account of the Russian Ministry of Defense to see firsthand the deluge of misinformation released by Moscow.[7] While the statement "Reality is whatever the Kremlin wants it to be" rang true long before Putin's invasion, propaganda coming out of wartime Russia seems to reach another level of distortion ("Russia's Top Five Persistent Disinformation Narratives"). From a democracy's perspective, it is astonishing that Russia – through the likes of its Defense Ministry, Russia Today, and Sputnik – can warp and augment reality however it likes for its information consumers.[8] Although many might hope that Western institutions built around the freedom of speech and press, equipped with resources like fact-checkers, may be immune to the torrent of Russian disinformation, there are inevitably cases in which some of that malign information sticks. As wartime Russia only increases its flood of propaganda, recruiting China into the process as it goes,[9] the future risk to the U.S. and its allies increases. Unfortunately, age-old wartime propaganda represents only the tip of the iceberg of what malign capabilities may look like in the future.

The real disinformation threat runs much deeper. Although Putin has used fake videos since he annexed Crimea in 2014, the expansion of deepfake technology in the late 2010s provides a new depth to visual disinformation. Deepfakes, like ones depicting Zelensky's surrender, are proliferating across the internet. While, currently, deepfakes are often crude in appearance and used chiefly in entertainment, the Russia-Ukraine conflict exhibits their grave political potential. Concerning a fake Zelensky video, author Nina Schick comments, "'Even though this video was really bad and crude, that won't be the case in the near future.' It would still 'erode trust in authentic media' [causing] 'People start to believe that everything can be faked…' 'It is a new weapon and a potent form of visual disinformation - and anyone can do it'" (qtd. in Wakefield, 2022). Sale Lilly, a senior policy analyst at the RAND Corporation, is also concerned that deepfakes might "poison the well" of media information. In other words, as deepfakes proliferate, people will not know what to trust and may cease trusting news altogether. A breakdown of trust between citizens, the government, and private journalism will, in turn, lead to greater instability and disproportionately affect Western democracies founded upon principles of personal freedom.

[7] Curiously, the ministry's actual website, http://eng.mil.ru, has been blocked on U.S. and most Western internet servers.
[8] These latter two mentions, Russia Today and Sputnik, are both Russian state-owned news agencies known for perpetuating misinformation and government propaganda.
[9] See footnote 4 for examples.

Domestic Impact

Unfortunately, wartime propaganda, election interference, and deepfakes only represent a few aspects of misinformation out of a myriad of other issues. A 2016 social media campaign targeting Texans provides a direct and foreboding example of Russian reach into everyday American life. According to the Texas Tribune, "Heart of Texas, a [Facebook group] that promoted Texas secession, leaned into an image of the state as a land of guns and barbecue and amassed hundreds of thousands of followers. One of their ads on Facebook announced a noon rally… to 'Stop Islamification of Texas.' A separate [Facebook group], United Muslims of America, advertised a 'Save Islamic Knowledge' rally for the same place and time." (Allbright). Although Americans often celebrate the freedom of speech and right to peaceful assembly, as protected by the Constitution, these social media pages were not American and did not intend to promote peaceful civic action. According to the book *Spies, Lies, and Algorithms*, the protests were manufactured by the Kremlin's Internet Research Agency through the creation of two respective Facebook groups. These groups collectively gained over five hundred thousand followers, which speaks legions to what Russian disinformation campaigns are capable of (Zegart). Not only did thousands of viewers fall for the elaborate ruse, but so did Facebook, the country's largest social media platform. The worst, and perhaps most dangerous part: protestors actually showed up.

"On May 21, 2016, Houston's Islamic Da'wah Center became the site of two dueling protests:" one anti-Islamization and white supremacist, the other Muslim (Zegart). The outcome was as one would expect. While only about sixty of these internet followers actually attended the artificial protests, they were armed with inflammatory posters, one AR-15, and a mysterious bubble machine (Glenn). It is easy to see, despite the police presence at this event, how quickly tensions could have risen to a breaking point and turned violent. Imagine if instead of 60, there had been 600. Suddenly, what was once Russian misinformation could turn into an indirect, violent attack on American soil. With recent surges in party polarization, protests-turned-riots, and mass shootings, the potential exploitative dangers of malign disinformation only rise.

Fortunately, many internet and social media platforms are now proficient at combating spam and misinformation – like the fake Russian Facebook groups.[10] However, as the torrent of spambots increases, so too will anti-misinformation technology need to progress. Additionally, as billionaires like Elon Musk begin to co-opt social media giants and advocates call for platforms like Web 3.0, social media and the internet face potential regression in their anti-misinformation and moderating capabilities.[11]

[10] That said, fact-checking technologies still has much room for growth. Social media platforms and third parties currently lack the capacity to crack down on foreign language misinformation (Hsu). The United States' vast Spanish-speaking populations are particularly vulnerable as most software can only analyze material written in English.

[11] Web 3.0, also known as Web3, is a new form of internet emerging from the same vein of blockchain technology and cryptocurrencies. It is inherently decentralized and does not need government oversight or big business intervention to operate (Ashmore, 2022).

International Impact

Another recent and prevalent Russian campaign is the spreading of disinformation, claiming "that the United States and Ukraine are conducting chemical and biological weapons activities in Ukraine" (Price). As Price points out, such a tactic is likely a lame attempt to justify Russian action in the region - illustrating another form that disinformation can take: justifying war. It is known that government officials sometimes resort to deception to garner public support for an issue. To do so in the past, they may invite or "manufacture an 'incident' that could be used to justify hostilities," as President Franklin D. Roosevelt may have done prior to entering World War II (Schuessler, 2010). Now, officials can bypass the hassle of covertly orchestrating a strategic sham and instead easily craft one from thin air with nothing more than a Tweet. The fact that actors like Putin can justify warfare with just a few fudged news articles should be alarming to the United States, its intelligence community, and any allied democracy.

So far, misinformation campaigns enacted by China have mainly targeted Taiwan and domestic regions (Harold et al.). In March 2022, Chinese outlets amplified the false Russian story of U.S. biological weapons in Ukraine and have aided its northern neighbor by spreading Russian propaganda since the conflict began (Bandurski). China also distributed a similar but distinct version of the falsified bioweapon report. In one of its first significant disinformation attacks directly targeting the United States, the Publicity Department of the Chinese Communist Party published across its several platforms articles alleging South Korean outcry against the presence of illegal U.S. bioweapon laboratories in Busan.[12] While independent fact-checkers quickly debunked these articles, such disinformation can increase strains on U.S.-South Korea relations and paint the U.S. in a bad light for other countries in the region – especially those under an authoritarian regime, who may already find themselves at odds with Western democracies.

The real concern here, however, is not the damage that this singular news story could incur but rather the precedent it creates. China has yet to "[carry] out substantial disinformation attacks on other U.S. allies or partners" (Harold et al.). Attacks like this falsified story and continued COVID-19 misinformation suggest a paradigm shift in China's policy. While the U.S. and its allies may be able to push back against the tide of information coming from Russia, if China continues to ramp up its disinformation operations in conjunction with its northern neighbor (which it expresses a desire to match), then this poses a much more substantial threat. A distorted pro-authoritarian, anti-West, Russo-China information reality in that hemisphere could pose significant problems for future Western relations across Asia, Eastern Europe, and Africa.

Disinformation and the Intelligence Community

Inside the intelligence community, disinformation provides a particular challenge for open-source intelligence (OSINT). On the one hand, OSINT is incredibly and "increasingly important to analysis owing to the information explosion in the internet age" (qtd. in George et al.). As the

[12] This was one of the articles highlighted in the introduction. See https://tinyurl.com/ChinaDaily-disinfo or https://tinyurl.com/Xinhua-disinfo for examples.

internet, social media, and availability of public information exponentially increase, so does the material from which an intelligence analyst may draw. However, OSINT is a double-edged sword. Given the recent deluge of information, including misinformation, analysts face "a major challenge… filtering for quality, usefulness, and authenticity" (qtd. in George et al., 2014). Sorting through open-source information is already tedious enough, coupled with the insidious threat of disinformation, and it can become an intelligence nightmare.

As China is in the early stages of large-scale disinformation campaigns and Russia is still tinkering with its operations, the United States and its allies must strike while the iron is hot. Unfortunately, The U.S. Intelligence Community has done little to push back against the challenge of foreign disinformation. Instead, social media companies, news media, and private citizens appear to have done the most to tackle disinformation and fake news entering the United States. Social media and other technology companies have begun instituting anti-misinformation programs to prevent the spread of falsified information. Many news outlets have begun fact-checking and refuting fake news. Private websites (a famous example being Snopes) and individuals have also made it their duty to track down misinformation across the news and social media. While these defensive measures are helpful, they lack IC involvement and are arguably all reactive responses.

IC Response

The threat posed by disinformation campaigns is significant and growing; however, there are ways in which the U.S. and its Intelligence Community can take proactive steps to prevent and mitigate future damage. The IC should work closely with private technology and social media companies to develop better ways of combating malign influence. Not only can AI technology be used to block spambots, fake news outlets, or misinformation torrents from reaching news and social media consumers, but it can also be used on the intelligence side to better sift through open-source information – increasing the effectiveness of OSINT. Agencies like the Federal Bureau of Investigation (FBI) can also partake in educational campaigns to bring awareness to the average American regarding the threat of disinformation. Lastly, as election interference has increased drastically in the past decade, the IC should focus more on decreasing malign foreign influence there. The U.S. may even learn several strategies from election security to apply against disinformation as a whole.

Election Security and France

Election security is vital to a healthy democracy and a national security issue. Interfering with Western elections is one of the most common ways in which Russia tries to destabilize and discredit its rivals, and it is an issue that will only increase in the future. Following problems with tampering in the 2016 and 2020 presidential elections, the U.S. government and Intelligence Community can look to France as an example of how to successfully counter foreign interference. In 2017, France held its own presidential elections, which malign foreign actors, namely Russia,

also attacked. However, despite successful interference in the U.S. election and others like the Brexit referendum, Russian interference in France largely failed due to effective countermeasures. Realizing the risk foreign actors could play in the democratic process following the U.K. and U.S. incidents, France quickly adapted and enforced many successful changes to preempt any interference. Such measures included supporting campaign and electoral watchdogs, raising awareness, diplomatic signaling, ending electronic voting, pressuring news and social media, maintaining transparency, creating counterintelligence, enabling law enforcement, blocking foreign propaganda outlets, and retaliating (Conley and Jeangène Vilmer).

While this long list holds recommendations for the U.S. federal government and future campaigns as a whole, the Intelligence Community can also focus on a few specific goals. Like it did before Putin invaded Ukraine, the Intelligence Community should signal its resolve to counter foreign interference and spread awareness thereof. France made sure to do this by "[alerting] the media, political parties, and the public" to the potential for disinformation and cyberattacks while also signaling to foreign powers its determination to prevent manipulation (Conley and Jeangène Vilmer). Such actions proved successful for the French in 2017, and similar action taken by the U.S. Intelligence Community to warn partners of Russian activity also worked.

Another ingenious tactic pursued by the Macron campaign in 2017 was to engage in "digital blurring" – a form of preemptive counterintelligence that exposed foreign hackers to a deluge of fake information and false flags (Conley and Jeangène Vilmer). While the U.S. Intelligence Community cannot actively counter-phish for campaigns, it can teach them how to successfully counter-phish, as such procedures are already standard in state counterintelligence (Johnson and Wirtz, 263-265). It is also essential that members of the IC remain vigilant against disinformation campaigns, especially ones targeting elections, and work to enable the Department of Homeland Security (including its Cybersecurity and Infrastructure Security Agency (CISA)) and FBI to identify, halt, and prosecute foreign threats. Lastly, the U.S. Intelligence Community can learn from the French model by working in conjunction with social media companies to identify and block fake sites, profiles, and information online. The same can be accomplished by pressuring news media to block the dissemination of misinformation and by discrediting known propaganda machines like Sputnik or China Daily. President Emmanuel Macron's re-election in 2022 (which went largely without a hitch) suggests that France again succeeded in stymying foreign interference and support for Russian apologist and far-right candidate Marine Le Pen.

Concluding Remarks and Recommendations

If the U.S. does nothing to combat disinformation, it will likely see the same problems it has seen in the past, such as electoral interference and continued anti-West campaigns. Russian and rising Chinese disinformation will continue sowing discord and distrust in the American public and its allies. Incidents like the 2016 Houston Islamic Da'wah Center protests could quickly become more frequent and violent. Additionally, public officials could become more prone to cyberattacks as foreign actors attempt to erode American trust in their leaders. While these threats are worrisome, future concerns are even worse. As deepfake technology progresses, separating truth from fiction will become more difficult. Scenarios can easily be imagined where deepfake content may evolve from the demoralizing (like Zelensky's "surrender") to the outright dangerous: imagine the chaos

if a video of a popular official was released, imploring rioters to storm a government institution in order to halt a cabal. Eventually, it is likely that trust in any form of visual media will seriously erode. However, this may not come before some severe damage is incurred upon the public or political institutions. Further, instead of "conquering" OSINT, the sea of information may become even more unnavigable for analysts seeking truth. The future risks of disinformation are not ones that the U.S. can ignore. Because of this, the government and IC must act before it gets swept behind.

The U.S. government should dedicate a more extensive budget toward anti-misinformation. In regard to safeguarding national elections, the U.S. should better fund and expand the role of the Federal Election Commission (FEC) and CISA to mirror that of the more robust National Commission for the Control of the Electoral Campaign for the Presidential Election (CNCCEP) and National Cybersecurity Agency (ANSSI) of France. The bolstering of these two election watchdogs would significantly help prevent election interference in the long run. Funding other initiatives, such as public awareness campaigns and close cooperation with technology and social media firms, is also necessary to ensure that the public and government are up-to-date on anti-misinformation measures. Only then, with these proactive programs, can trust begin to be restored in the heart of American information.

The unique threat that disinformation poses to Western democracies and their partners is nothing new. Russia and its Soviet predecessor have levied significant campaigns against the United States since the 1980s. Despite their age, disinformation campaigns have drastically increased in volume and capabilities in recent years, posing a significant future risk for the U.S. and its allies. As Russia becomes more emboldened and the threat of disinformation becomes even more realized with the addition of China and improved technology into the mix, the U.S. and Western democracies must act to preserve the freedom of truth before it is too late.

References

Allbright, Claire. "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest." *The Texas Tribune*, The Texas Tribune, 1 Nov. 2017, https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-l/.

Ashmore, Dan. "A Brief History Of Web 3.0." Edited by Farran Powell, *Forbes*, Forbes Magazine, 9 Jan. 2023, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-web-3-0/.

Bandurski, David. "China and Russia Are Joining Forces to Spread Disinformation." *Brookings*, The Brookings Institution, 11 Mar. 2022, https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spread-disinformation/.

Bremmer, Ian, and Cliff Kupchan. "Risk 5: Russia." *Top Risks 2022*, Eurasia Group, 3 Jan. 2022, https://www.eurasiagroup.net/live-post/top-risks-2022-5-Russia.

Clark, Robert M. *The Technical Collection of Intelligence*. CQ Press, 2011.

Conley, Heather A., and Jean-Baptiste Jeangène Vilmer. "Successfully Countering Russian Electoral Interference." *CSIS*, Center for Strategic and International Studies, 21 June 2018, https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

Ellick, Adam, and Adam Westbrook. "Operation InfeKtion: Russian Disinformation: From Cold War to Kanye." *The New York Times*, The New York Times, 13 Nov. 2018, https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html.

George, Roger Z., et al. "Is Intelligence Analysis a Discipline?" *Analyzing Intelligence*, Georgetown University Press, Washington, DC, 2014.

Glenn, Mike. "A Houston Protest, Organized by Russian Trolls." *Houston Chronicle*, Hearst Newspapers, 19 Feb. 2018, https://www.houstonchronicle.com/local/gray-matters/article/A-Houston-protest-organized-by-Russian-trolls-12625481.php.

Goldstein, Josh A., and Shelby Grossman. "How Disinformation Evolved in 2020." *Brookings*, The Brookings Institution, 4 Jan. 2021, https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020/.

Gordon, Sue, and Eric Rosenbach. "America's Cyber-Reckoning." *Foreign Affairs*, Council on Foreign Relations, 2022, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

Harold, Scott W., et al. *Chinese Disinformation Efforts on Social Media*, RAND Corporation, Santa Monica, CA, 2021, https://www.rand.org/pubs/research_reports/RR4373z3.html.

Hsu, Tiffany. "Misinformation Swirls in Non-English Languages Ahead of Midterms." *The New York Times*, The New York Times, 12 Oct. 2022, https://www.nytimes.com/2022/10/12/business/media/midterms-foreign-language-misinformation.html.

Johnson, Loch K., and James J. Wirtz. *Intelligence: The Secret World of Spies: An Anthology*. 5th ed., Oxford University Press, 2019.

Lilly, Sale. "Intelligence and Think Tanks." INTS 452.01, 21 Apr. 2022, Malibu, CA, Pepperdine University.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. CQ PRESS, 2009.

Paul, Christopher, and Miriam Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." *RAND Corporation*, 2016. *Perspectives*, https://doi.org/10.7249/pe198.

Price, Ned. "The Kremlin's Allegations of Chemical and Biological Weapons Laboratories in Ukraine." *Office of the Spokesperson*, U.S. Department of State, 9 Mar. 2022, https://www.state.gov/the-kremlins-allegations-of-chemical-and-biological-weapons-laboratories-in-ukraine/.

"Russia's Top Five Persistent Disinformation Narratives." *Office of the Spokesperson*, U.S. Department of State, 20 Jan. 2022, https://www.state.gov/russias-top-five-persistent-disinformation-narratives/.

Severance, Hayley, and Jacob H. Eckles. "Russian Propaganda Establishes a Dangerous, Permissive Environment." *NTI*, The Nuclear Threat Initiative, 11 Mar. 2022, https://www.nti.org/atomic-pulse/russian-propaganda-establishes-a-dangerous-permissive-environment/.

Schifrin, Nick, and Adam Ellick. "The Long History of Russian Disinformation Targeting the U.S." *PBS Newshour*, PBS, 21 Nov. 2018, https://www.pbs.org/newshour/show/the-long-history-of-russian-disinformation-targeting-the-u-s.

Schuessler, John M. "The Deception Dividend: FDR's Undeclared War." *International Security*, vol. 34 no. 4, 2010, p. 133-165. *Project MUSE* http://muse.jhu.edu/article/377380.

United States, Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence, 7 Feb. 2022. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

Wakefield, Jane. "Deepfake Presidents Used in Russia-Ukraine War." *BBC News*, BBC, 18 Mar. 2022, https://www.bbc.com/news/technology-60780142.

Zegart, Amy B. "Decoding Cyber Threats." *Spies, Lies, and Algorithms: The History and Future of American Intelligence*, Princeton University Press, Princeton, NJ, 2022, pp. 251–254.