ABSTRACT

Western private sector companies are vulnerable to malign disinformation attacks by nation-state actors, including Russia and China. Vulnerability to disinformation may vary by industry and other factors; however, health-related organizations and public health issues have long been targets. During the development of vaccines against COVID-19, both Russia and China attacked both the efficacy of mRNA vaccines and the companies that developed them. During the 1980s, Russia conducted *Operation Infektion*, a disinformation campaign about the HIV/AIDS epidemic, linking it to an attack against Black populations worldwide. The onset of the Russian invasion of Ukraine detected a sudden shift as Russian disinformation shifted from vaccines to Ukraine in a seemingly coordinated fashion. This shift may have indicated the Russian state's direction to disinformation originating from there.

At the onset of the Russian invasion of Ukraine, the Western states began imposing a series of sanctions regimes against Russia with varying levels of support from the private sector. As of mid-June 2022, over 900 companies worldwide provided substantial support to the sanctions against Russia. Three hundred twenty-five companies had halted operations in Russia or had exited completely. Of these, about half were U.S. or U.K. companies, with 116 and 45 respectively. Additional strong supporters of the sanctions included Germany (23), France (21), and Poland (21).

Both the numerous companies supporting economic sanctions, as well as those not supporting, may become targets of malign information campaigns. Recent articles in Sputnik International included reporting on the reopening of McDonald's under Russian ownership and an incident in the United States where a Muslim family was served fish sandwiches with bacon. State media reporting on Starbucks included management efforts against unionization. Private sector companies may become the new targets of malign information campaigns to cause harm to the companies and Western nations.

Team Members

MEMBERS	COMPANY/AGENCY
Champion: Dana LaFon	**NSA**
Champion: Trisha Ripley	**ODNI**
Alexandra Armstrong	**American Express**
Michael Ficht	**FBI**
Wesley Moy	**Johns Hopkins University**
Taylor Price	**Dell Technologies**
Janice Rosado	**NSA**
Eric Schorr	**Snap Inc.**
Christine Sublett	**Sublett Consulting, LLC.**
Kimberly Young	**DHS/I&A**

Introduction

Leveraging virtual interviews and open-source research and analysis, this paper examines the vulnerability of Western private sector companies to malign disinformation attacks by nation-state actors, including recent narratives deployed in Eastern Europe that may leverage against the West. Historic disinformation attacks, including *Operation Infektion*, in which the Soviet Union waged a disinformation campaign in the 1980s about the global HIV/AIDS epidemic, alleging it originated in a US military lab, are examined.

This paper evaluates recent disinformation efforts, including Russian, Chinese, and nation-state affiliated campaigns to undermine confidence in mRNA vaccines and the companies that developed them. It looks at the rapid pivot in Russian disinformation from anti-vaccine campaigns to anti-Ukraine narratives following their further invasion of Ukraine in February 2022, indicating potential Russian state direction of malign influence efforts. Traditional cyber threat actors, attack vectors, and recent cyber activity perpetrated by nation-states including Russia and China, nation-state affiliated, and criminal organizations against U.S. critical infrastructure and the West are explored and evaluated. Lastly, the paper examines the impact of the curtailing of business or withdrawal of over 1000 companies out of the Russian market in support of economic sanctions, including the extent to which these companies have become targets of malign influence campaigns. With a specific focus on the Eastern European context as a Petri dish for disinformation campaigns, this paper warns of emerging malign influence tactics, techniques, and narratives that may be leveraged against the private sector in the West.

[1]

China and Russia view the United States as their main adversary and seek to diminish its influence when possible.[2] However, their underlying motivations differ significantly, and the differences determine national objectives and the strategies selected to realize those objectives. Disinformation attacks potentially support foreign state national objectives.[3] Russia and China are good examples of contrasting national objectives that can serve through malign influence campaigns. The Russian leadership perceives Western democracy as the greatest threat and seeks to attack Western democracies and undermine its institutions.[4] In contrast, China aims to be the preeminent power in Asia in the near term and, in the longer term, lead the world in economic, military, and political power.[5] [6] These objectives, while dissimilar, can both be served through disinformation used in conjunction with other instruments of national power.

---

[1] McCorkindale, T. (2019) How responsible are social media platforms for spreading and fixing disinformation? State of Digital Publishing. Retrieved from https://www.stateofdigitalpublishing.com/opinion/social-media-responsibility-for-spreading-and-fixing-disinformation/.

[2] Miller, A. and Sololsky, R. (2021) Biden is right that global democracy is at risk. But the threat isn't China. *The Washington Post*. Retrieved from https://www.washingtonpost.com/outlook/democracy-summit-china-russia/2021/12/03/d64d4544-537a-11ec-8769-2f4ecdf7a2ad_story.html.

[3] Biden, J. And Carpenter, M. (2018) How to Stand Up to the Kremlin: Defending Democracy Against Its Enemies. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/russia-fsu/2017-12-05/how-stand-kremlin.

[4] ibid.

[5] Liu, Q. (2021). Important Tasks to be fulfilled in the next five years. *China Daily Global Edition*. Retrieved from https://global.chinadaily.com.cn/a/202103/06/WS6042d816a31024ad0baad375.html.

[6] Callahan, W. (2016) China 2035: from the China Dream to the World Dream. *Global Affairs*. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/23340460.2016.1210240.

CISA MDM Definitions

- Misinformation, disinformation, and malinformation make up what CISA defines as "information activities". When this type of content is released by foreign actors, it can be referred to as foreign influence.
- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.
- Foreign and domestic threat actors use MDM campaigns to cause chaos, confusion, and division. These malign actors are seeking to interfere with and undermine our democratic institutions and national cohesiveness.

US Department of Homeland Security/Cyber and Infrastructure Security Agency (CISA), https://www.cisa.gov/mdm

The U.S. Department of Homeland Security's Critical Infrastructure and Cyber Security Agency (CISA) describes malign information in terms of its truthfulness, or lack thereof, and whether or not it is intended to cause harm.

The power of disinformation against the private sector from state or state-sponsored campaigns must be understood from two perspectives. Disinformation is pervasive as private information is stolen and leaked for malicious purposes, wedges are driven into the discourse of liberal democracies, and perpetrators continue their efforts while denying their activities (Rid, 2020). First, from the threat perspective, the state's capability and intent. The cost of developing such a capability is almost negligible for a state actor.[7] Inaccurate information travels 10 to 20 times faster than accurate information.[8] Secondly, the vulnerability and consequences of such attacks must be considered. Disinformation attacks against governments and institutions are often highlighted, but the vulnerability to corporate reputation, brands, markets for goods and services, and financial markets are omitted.[9] Disinformation attacks by state actors include

[7] Condliffe, J. (2017) Fake News Is Unbelievably Cheap to Produce. MIT Technology Review. Retrieved from https://www.technologyreview.com/2017/06/14/151233/fake-news-is-unbelievably-cheap/.
[8] Dizikes, P. (2018) Study: On Twitter, false news travels faster than true stories. MIT News. Retrieved from https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.
[9] Ferraro, M. (2019) Disinformation is harming businesses. Here are 6 ways to fight it. *CNN Business*. Retrieved from https://www.cnn.com/2019/06/10/perspectives/disinformation-business/index.html.

fueling conspiracy theories about the health effects of 5G technology and mRNA vaccine efficacy and safety.[10] It is notable that while such attacks are currently uncommon, these two instances have become global and persistent.

Disinformation against the private sector has not been thoroughly explored, and new risks have appeared, making a highly uncertain environment in which coordinated disinformation attacks are a threat to brand equity and the safety of employees and customers.[11]

Russian Intent and Objectives

Russian efforts to undermine Western democracies and democratic institutions are not new. In February 2022, the U.S. Office of the Director of National Intelligence assessed that Russia would continue to present a formidable challenge to the United States and its allies as it aggressively pursued its interests or undermined the West.[12] The Post-Cold War assumption that economic engagement with Russia would bring peace and stability to Europe was hampered by the 2008 Global Recession and continued Russian use of its instruments of national power to undermine democratic institutions and legitimacy.[13] This Russian effort is not a new development but a continuation of a decades-long effort by the Soviet Union and later Russia to undermine democratic legitimacy throughout the world.[14]

Russia uses its intelligence agencies, surrogates, and a wide-ranging set of tools to increase its influence, undermine Western alliances, and attack the United States by degrading its global standing, stoking internal discord, and influencing internal decision-making.[15] The United States failed to realize the long-standing and severe nature of the Russian disinformation campaign until the 2016 presidential election. Even then, national security experts failed to realize how disinformation undermined democratic ideals.[16] The Soviet Union, followed by

---

[10] Jain, L. (2021) Disinformation is emerging as a threat to businesses. *Fast Company*. Retrieved from https://www.fastcompany.com/90633225/disinformation-threat-business.

[11] Sohn, A., Goldenberg, A., Paresky, P., Early, O., Marchi, L., Gps, M., and Finkelstein, J. (2021) *The Future of Disinformation Operations and the Coming War on Brands*. Network Contagion Research Institute. Rutgers University.

[12] Office of the Director of National Intelligence(ODNI) (February 2022). *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC.

[13] Center for Strategic and Internatioal Studies (CSIS) (June 2015). *Made in China 2025*. Retrived from www.CSIS.org/analysis/made-in-china-2025.

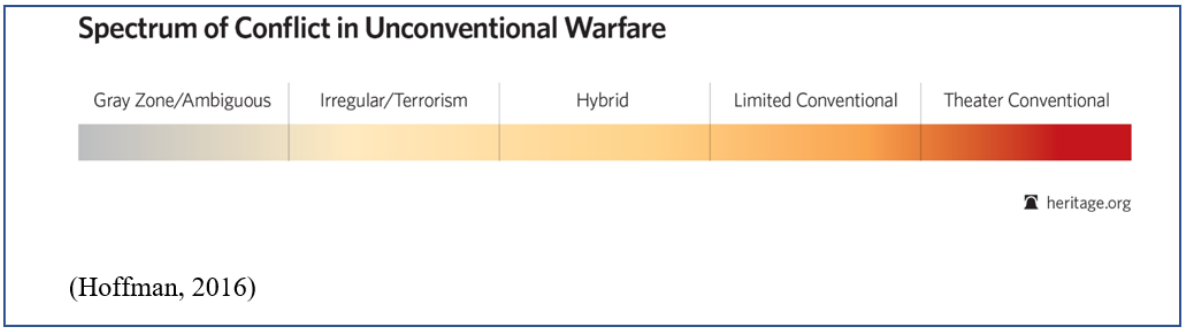
[14] Moy, Wesley and Kacper Gradon. (December, 2020) COVID-19 Effects and Russian Disinformation. *Homeland Security Affairs* 16, Article 8 www.hsaj.org/articles16533.

[15] ODNI, 2022.

[16] Murphy, B. (2022) Decaying National Security and the Rise of Imagined Tribalism. *The RUSI Journal*. DOI: 10.1080/03071847.2022.2072763.

Russia, has waged a decades-long campaign against the United States and its Western allies to conduct ideological subversion to undermine democracy and democratic institutions.[17] The Russian Chief of General Staff Valery Gerasimov posited in 2013 that non-military means had exceeded the utility of military force in a conventional conflict with malign influence campaigns, including propaganda, misinformation, and disinformation affecting the wills, thoughts, and beliefs of adversary populations.[18]

FIGURE 1

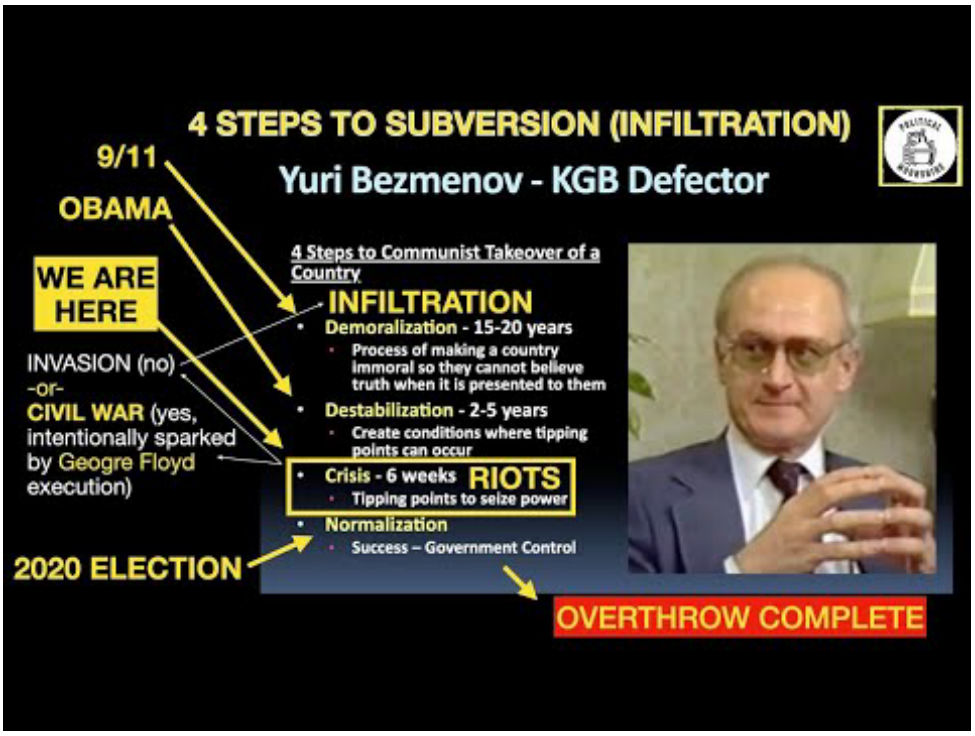


(Hoffman, 2016)

[19]

According to KGB defector Yuri Bezmenov, there are four phases to Russian ideological subversion: First, demoralization spanning 15 to 20 years; second, destabilization spanning 2 to 5 years; third, crisis spanning just weeks; and then normalization, which consolidates the new ideology.[20] Malign information campaigns would support all phases of subversion campaigns but be especially important in the prolonged first two.

[17] Bezmenov, Y. (1984) Former KGB Agent, Yuri Bezmenov, Warns America About Socialist Subversion. Youtube. Retrieved from https://www.youtube.com/watch?v=yErKTVdETpw.
[18] Moy & Gradon, 2020.
[19] Hoffman, 2016.
[20] Charles River Editors (2020) Yuri Bezmenov: *The Life and Legacy of the Influential KGB Informant Who Defected to the West*. Kindle Unlimited Edition.



[21]

The Russian leadership has long believed that the Western democracies, namely the United States, work to undermine Russia, weaken Putin, and spread its influence to the former Warsaw Pact countries and Russian republics.[22] Russia uses Poland and other former-Warsaw Pact countries as a testing ground for its cyber and disinformation tactics and campaigns.[23]

Putin wants to shift attention away from internal weaknesses, including corruption and the poor economy.[24] In 2020, the Russian economy was estimated to be about $1.5 trillion, the 11th largest in the world; however, on a per capita basis, it was ranked 64th at just $11,654.[25] Poor conceptualization and execution have fizzled plans to bolster economic growth.

Chinese Intent and Objectives.

China is the primary threat to U.S. competitiveness in technology and is willing to use numerous tools to advance its capabilities, including espionage, acquisitions, and trade policy, to

[21] Bezmanov, 1984.
[22] ODNI, 2022.
[23] Moy & Gradon, 2020.
[24] Biden & Carpenter, 2018
[25] Statistics Times (2021). *World GDP Ranking 2021*. Retrieved from https://statisticstimes.com/economy/projected-world-gdp-ranking.php.

achieve advantages.[26] China uses a multi-pronged effort to undermine democracy and its institutions, create and exploit doubts about U.S. leadership, and extend its influence to highlight the United States failures and hypocrisy.[27] The United States continues to lead in overall power in Asia. However, China also holds a superpower status measured by its regional influence and resources. In the region, China leads the United States in economic capability and economic relationships.[28] Xi Jinping, observing the United Kingdom's withdrawal from the European Union and the election of populist Donald Trump as United States president, perceived that the West's leading democracies were withdrawing from the international order and facing domestic governance issues.[29]

When investigating its motives and aspirations, it is essential to understand China's geo-economic ambitions.[30] The description of Chinese aspirations to become Zhongguo (中國/中国) or the Middle Kingdom potentially distorts perceptions of its grand strategy. Perhaps a better way to describe China's goal would be the "Central Country" of the world. China aspires to lead the world in all aspects of national power, diplomatic, informational, military, and economic, by 2035.[31] [32] China is on track to become not just another big player but the most significant economic player in the history of the world.[33] There are unambiguous signs that China seeks to contest the United States' global leadership.[34]

The former director of the Brookings Institution's China Strategy Initiative, Rush Doshe, has charted China's grand strategy to regain what it perceives as its central role in the world.[35] That strategy first required China to blunt the United States' influence over its actions which has largely been accomplished. The second is to assert Chinese influence regionally, diplomatically, with information, militarily, and economically. Finally, China wants to extend its power globally

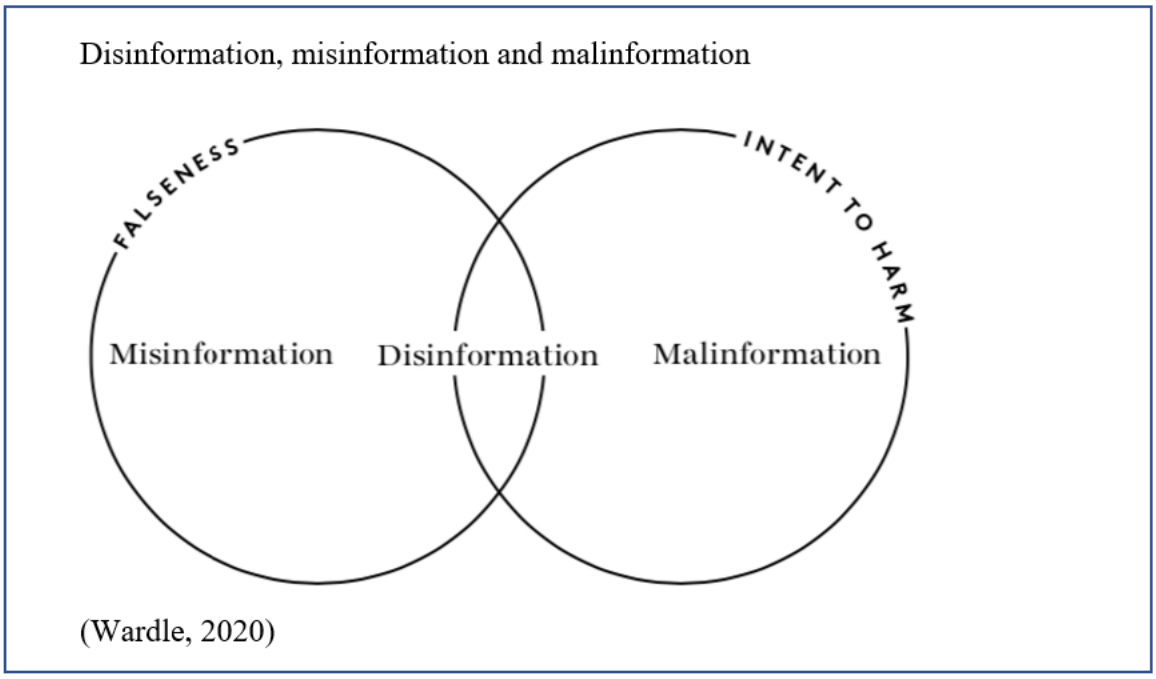
[26] ODNI, 2022.
[27] ODNI, 2022.
[28] Lemahieu, H. and Leng, A. (2021) Asia Power Index: Key Findings 2021. Lowy Institute. Retrieved from https://power.lowyinstitute.org/.
[29] Doshi, R. (2021) *The Long Game: China's Grand Strategy to Displace American Order*. Oxford University Press. New York, NY.
[30] Jain, 2020.
[31] Liu 2021.
[32] Callahan 2016.
[33] Allison, 2017.
[34] Sullivan, J. And Brands, H. (2021) China Has Two Paths To Global Domination. Carnegie Endowment for International Peace. *Foreign Policy*. Retrieved from https://carnegieendowment.org/2020/05/22/china-has-two-paths-to-global-domination-pub-81908.
[35] Doshe, 2021.

and displace the United States as the most influential country. Made in China 2025 is an aggressive plan to upgrade Chinese productivity in many industries, emphasizing robotics, artificial intelligence, and advanced computing.[36] China could choose a path in which economic and technological power are more important than military power in its quest for global leadership.

The Malign Information Environment

In November 2021, John Cohen, then DHS Under Secretary for Intelligence & Analysis, warned of the disinformation efforts being conducted by foreign intelligence agencies that agitated domestic extremists.[37] U.S. strategic culture conceptualizes war and peace as two separate and distinctive states. In contrast, the reality is that conflict exists along a spectrum and includes all of the instruments of national power, including information.[38] Thomas Rid described four waves of disinformation. Beginning in the 1920s and 1930s, it was a weapon of the weak, often aimed at the United States and the Soviet Union. Following World War II, American intelligence was at the forefront with aggressive and unscrupulous information under the guise of political warfare. At the same time, the USSR and its allies used the term disinformation for their activities. In the 1970s, the Eastern Bloc countries became more proficient than the West and the term active measures, capturing a broad range of activities, came into use. The fourth wave saw the widespread adoption of technology and the Internet with even more activities, perhaps less measured.[39]

[36] Crawford, E. (2019) Made in China 2025: The Industrial Plan that China Doesn't Want Anyone Talking About. *PBS Frontline*. Retrieved from https://www.pbs.org/wgbh/frontline/article/made-in-china-2025-the-industrial-plan-that-china-doesn't-want-anyone-talking-about/.
[37] Selden, J. (2021) Foreign Disinformation Stokes Fears of Violence in US. Voice of America News. Retreived from https://www.voanews.com/a/foreign-disinformation-stokes-fears-of-violence-in-us/6356904.html.
[38] Hoffman, F. (2016) The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War. *Military Strength Topical Essays*. The Heritage Foundation. Retreived from https://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protracted-gray.
[39] Rid, T. (2020) *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux. New York.



Social media algorithmic filtering and prioritization emphasize increased user engagement over content truthfulness. Facebook recognized in 2018 that its algorithms would emphasize divisive content and exploit human attraction to divisiveness.[40] This design feature directly supports Russian active measures to splinter democracies.

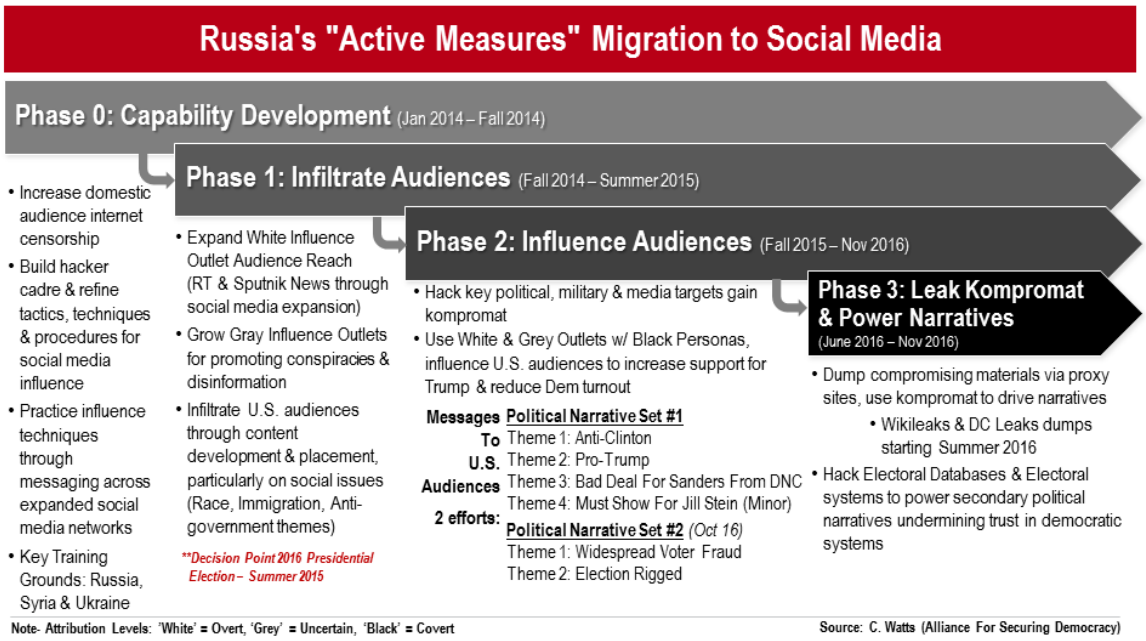
The year 2020 saw the worldwide emergence of black public relations (P.R.) firms able to field fake online user accounts, promote false narratives, and false news outlets to manipulate online discourse. Peng Kuan Chin, the principal of a black P.R. firm in Taichung, Taiwan, stated that the software his firm uses is designed to operate against Facebook and the strong demand for these services.[41]

Past Activities - Active and Asymmetric Measures

The world has witnessed a stratospheric rise in references to disinformation campaigns, mainly since the 2016 U.S. Presidential campaign. Still, going even further back, it can be traced to the ubiquitous nature of social media. However, historians have argued that disinformation or

[40] Congressional Research Service (CRS) (2021) *Social Media: Misinformation and Content Moderation Issues for Congress* R46662. Retrieved from https://crsreports.congress.gov.
[41] Silverman, C., Lytvynenko, J., and Kung, W. (2020). Disinformation For Hire: How A New Breed of PR Firms Is Selling Lies Online. *Buzzfeed*. Retrieved from https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms.

"active measure" campaigns can be traced back centuries. With the ever-increasing rise in global connectivity, the amount of disinformation your average citizen is exposed to daily has exploded. The COVID-19 pandemic only exacerbated the already dizzying rise in disinformation narratives spreading globally and injected a host of new conspiracies to be projected by foreign and domestic actors onto the global population. However, the explosive growth in disinformation narratives by foreign states regarding COVID-19's origins, treatment, and vaccinations also has a recent historical parallel, known as *Operation Infektion or Operation Denver*.



[42]

In the early 1980s, a very different global pandemic was only beginning to be noticed by doctors and research scientists. Still, even as it began to spread rapidly in the United States among the gay community, much about it remained understood.[43] Going into this void, as conspiracy theories started to percolate in some small newspapers and magazines as to the origins of the Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS), the USSR recognized an opportunity to initiate a disinformation campaign, building on skepticism and conspiracy theories that already existed in the West.

Operation Infektion has been described as "…as one of the most tenacious conspiracy theories to have arisen in the twentieth century, and it continues to spread today, especially

[42] Watts, C. (2018) Russia's Active Measures Architecture: Task and Purpose. Alliance for Securing Democracy. Retrieved from https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/.
[43] Selvage, Douglas E., "Operation "Denver": The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985-1986 (Part 1)", *Journal of Cold War Studies*, October 2019.

throughout the internet".[44] As noted, conspiracy theories around the origins of HIV were already beginning to appear in some newspapers in the early 1980s in the U.S. and abroad, including in an Indian newspaper, the Patriot. Still, it was not until 1985 that the KGB began to join the fray.[45]

46

In 1985, Bulgarian intelligence received a memo from the KGB requesting their assistance in promoting the false narrative that the U.S. military at Fort Detrick, Maryland, had developed HIV.[47] From that point forward, the KGB utilized a variety of actors, both under their control, as well as witting and unwitting actors in the West, to seed this narrative, to the point where it reached the mainstream press, including appearing in the tabloid press in the U.K. and a segment on CBS News with Dan Rather.[48]

While the intricacies of the KGB's efforts to seed this narrative are wide-ranging, including the promotion of false scientific papers by an East German scientist, it reached an enormously broad audience, ranging from African American newspapers in the United States to

[44] ibid.
[45] ibid.
[46] Fact Republic (2018) 40 Interesting Government and Military Operations. Retrieved from https://factrepublic.com/40-interesting-government-and-military-operations/2/.
[47] Selvage, Douglas & Christopher Nehring, "Operation "Denver": KGB and Stasi Disinformation Regarding AIDS"; Sources and Methods - Wilson Center, 22 July 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids.
[48] Selvage and Nehring, 2020.

senior members of governments in Africa.[49] While the Soviet Union ultimately disavowed the AIDS "active measure" under pressure from the U.S., the damage had been done.[50] Since, *Operation "Infektion,"* Russian disinformation actors have in recent years chosen to recycle components of *Operation Infektion* when promoting false narratives surrounding the origin of diseases such as Ebola, as well as the sinister nature of the U.S. military bio-labs when trying to blame U.S. and Western researchers for diseases to include COVID-19.[51]

Disinformation and COVID-19

When the COVID-19 pandemic first appeared in early 2020 in the People's Republic of China (PRC), very little was understood about it. However, since January 2020, while an enormous amount of energy has been devoted to understanding it from the scientific perspective, an equal amount of effort has been devoted by Russian and Chinese government-affiliated actors to promote disinformation surrounding its origins, treatment, and, almost immediately, potential vaccinations for it. However, the methods they chose to use, the disinformation narratives, and the targets of their disinformation campaign varied significantly.

[52]

China experienced its infodemic with COVID-19 misinformation, with Traditional Chinese Medicine often cited as effective remedies.[53] The origins of the COVID-19 pandemic have been

[49] Selvage, 2019.
[50] Rid, 2020.
[51] Selvage and Nehring,2020.
[52] Vaniotis, G. (2020) The Development & Function of mRNA Vaccines. Labtag|Blog. Retrieved from https://blog.labtag.com/the-development-function-of-mrna-vaccines/.
[53] Chen, K., Luo, Y., Hu, A., Zhao, J., & Zhang, L. (2021) Characteristics of Misinformation Spreading on Social Media During the COVID-19 Outbreak in China: A Descriptive Analysis. *Risk Management and Healthcare Policy* 14. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8121282/.

highly politicized, with the U.S. government advancing the lab leak theory while China spread information to counter criticisms.[54]

When the COVID-19 pandemic first appeared in early 2020 in the People's Republic of China (PRC), very little was understood about it. However, since January 2020, while an enormous amount of energy has been devoted to understanding it from the scientific perspective, an equal amount of effort has been devoted by Russian and Chinese government-affiliated actors to promote disinformation surrounding its origins, treatment, and, almost immediately, potential vaccinations for it. However, the methods they chose to use, the disinformation narratives, and the targets of their disinformation campaign varied significantly.

During the COVID-19 pandemic, China was the leader in spreading disinformation about the origin of the disease, reacting, in part, against then-President Donald Trump's labeling the disease the *China Virus*. [55] The Chinese government has advanced misinformation, including Zhao Lijian, deputy director of the Information Department of the Chinese Ministry of Foreign Affairs, who accused the U.S. Army of bringing the virus to Wuhan during the World Military Games in 2019.[56]

57

[54] Chen, E. (2021). Chinese COVID-19 Misinformation A Year Later. *China Brief*. The Jamestown Foundation. Retrieved from https://jamestown.org/program/15eijing-covid-19-misinformation-a-year-later/.
[55] Kinetz, E. (2021) COVID conspiracy shows the vast reach of Chinese disinformation. *Associated Press News*. Retrieved from https://apnews.com/article/beijing-media-coronavirus-pandemic-conspiracy-only-on-ap-e696b32d4c3e9962ac0bdbdae2991466.
[56] Chen, 2021.
[57] European Platform for Democratic Elections (2020) Kremlin's 10 Disinformation Narratives on COVID-19 in Georgia. Retrieved from https://www.epde.org/en/news/details/kremlins-10-disinformation-narratives-on-covid-19-in-georgia.html.

Before the pandemic, Facebook and Twitter removed accounts associated with Chinese state information campaigns.[58] Citizen journalists reporting on the pandemic from Wuhan disappeared because their reporting was counter to the official narrative. China promotes the narrative that its successes against COVID-19 prove that its political system is superior to Western democracy.[59]

Even as international organizations and national governments attempted to develop plans and procedures to address the COVID-19 pandemic and understand how it happened, various state-sponsored actors tied to the PRC government actively attempted to obfuscate and redirect allegations COVID-19 originated in China.[60] While Russia's various disinformation efforts related to COVID-19 were found to be varying, employing a variety of narratives and conspiracy theories, and tailoring their messaging to multiple groups, PRC disinformation and propaganda efforts were, on the whole, unified.[61] Specifically, "China-linked disinformation efforts focused on the origins of the virus and involved multiple conspiracy theories, such as the virus originated in the United States or one of its global bio-labs…" Generally, China's messaging frequently focused on protecting the country's image by calling into question the origins of COVID-19 and highlighting the government's response to it.[62]

China uses a network of media organizations to disseminate misinformation online at home and abroad. It produces misleading information on U.S. issues, including election voter fraud, COVID-19, and QAnon conspiracy theories.[63] Misinformation related to China and the COVID-19 pandemic included the Wuhan Institute of Virology as a secret biological weapons facility and the consumption of bats in China as a source of the disease.[64] China and Russia have actively created mistrust in Western COVID-19 vaccines, emphasizing safety concerns and

---

[58] Twigg, K. And Allen, K. (2021) The disinformation tactics used by China. *BBC News*. Retrieved from https://www.bbc.com/news/world-asia-china-55355401.
[59] BBC News (2020) China Covid-19: How state media and censorship took on coronavirus. Retrieved from https://www.bbc.com/news/world-asia-china-55355401.
[60] Virality Project, "Memes, Magnets and Microchips: Narrative Dynamics Around COVID-19 Vaccines"; Stanford Internet Observatory; 2022; https://purl.stanford.edu/mx395xj8490.
[61] Matthews, Miriam, Katya Migacheva, and Ryan Andrew Brown; "Superspreaders of Malign and Subversive Information on COVID-19: Russian and Chinese Efforts Targeting the United States"; Rand Corporation; 2021; https://www.rand.org/pubs/research_reports/RRA112-11.html.
[62] Matthews, Migacheva, & Brown, 2021.
[63] Graphika (2021) Ants in a Web: Deconstructing Guo Wengui's Online 'Whistleblower Movement.' Retrieved from https://graphika.com/reports/ants-in-a-web/.
[64] Evanega, S., Lynas, M., Adams, J., Smolenyak, K., & Insights, C. G. (2020). Coronavirus misinformation: quantifying sources and themes in the COVID-19 'infodemic'. *JMIR Preprints*, *19*(10), 2020.

promoting their vaccine's relative efficacy.[65] China remains nascent with mRNA technology, with just ten companies conducting research, lagging by 10 to 20 years compared to Western firms.[66] In 2020, two Chinese government-linked hackers attempted to steal mRNA technology from COVID-19 mRNA vaccine producer Moderna.[67]

In addition to China focusing its disinformation narratives around critical messages, they effectively maintained this messaging across various platforms. This included state-backed media, social media, and foreign policy establishment, mainly through Chinese diplomats described as "wolf warriors" for their aggressive social media presence, challenging research, and reports viewed as damaging to the Chinese government.[68] Unlike the Russian government's disinformation efforts, the Chinese government's initiatives focused on protecting China's global image rather than sowing discord in foreign countries.[69]

However, as China began to roll out its vaccines to combat COVID-19, Sinopharm, and Sinovac, Chinese actors shifted some of their focus to other vital narratives.[70] Even as China publicly promised to share their vaccine with the world at a reasonable price, research began to be released indicating they were not as effective as Pfizer and other Western-developed vaccines .[71] As a result, China and Chinese-government-backed actors began to actively highlight any real or imagined issues with Western-backed vaccines, including whether they were dangerous.[72] In addition, China continued to focus on its other vital narratives, questioning the origins of COVID-19, highlighting China's effective response to the virus, and continuing to pass aspersions about Western developed vaccines. For example, throughout 2021, research showed that Chinese actors regularly tried to promote conspiracy theories regarding allegations that U.S.-

[65] Emmot, R. (2021) China Russia, China sow disinformation to undermine trust in Western vaccines: EU. *Reuters*. Retrieved from https://www.reuters.com/world/china/17eijin-china-sow-disinformation-undermine-trust-western-vaccines-eu-report-says-2021-04-28/.
[66] Huang, J. (2021) Chinese drugmakers play catch up on mRNA vaccines amid pandemic. *S&P Global Market Intelligence*. Retrieved from https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/chinese-drugmakers-play-catch-up-on-mrna-vaccines-amid-pandemic-62527322.
[67] Bing, C. and Taylor, M. (2020) Exclusive: China-backed hackers 'targeted COVID-19 vaccine firm Moderna.' *Reuters Healthcare & Pharma*. Retrieved from https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl/exclusive-china-backed-hackers-targeted-covid-19-vaccine-firm-moderna-idUSKCN24V38M.
[68] Matthews, Migacheva, & Brown, 2021.
[69] Matthews, Migacheva, & Brown, 2021.
[70] Virality Project, 2022.
[71] Dubow, Ben, Edward Lucas, & Jake Morris; "Jabbed in the Back: Mapping Russian and Chinese Information Operations During the COVID-19 Pandemic"; Center for European Policy Analysis; 2 December 2021; https://cepa.org/jabbed-in-the-back-mapping-russian-and-chinese-information-operations-during-covid-19/.

[72] Virality Project, 2022.

based bio-labs, including Fort Detrick in Maryland, was responsible for the release of COVID-19.[73] This narrative, which may appear to be a carryover from Operation "Denver," was also embraced by Russian disinformation actors.

Russia

Since the outbreak of COVID, Russian actors, both those directly affiliated with the government and those acting covertly, have been focused on promoting a variety of disinformation narratives that have evolved as the world has adapted and responded to COVID. Like with Operation "Denver," Russian actors initially focused on calling into question the origins of COVID-19, recycling narratives from previous crises, but as CEPA noted, "…disinformation builds off existing, master narratives that Russia advances."[74] These efforts evolved, particularly with Russia's announcement of the Sputnik V vaccine in August 2020 and the Russian government's desire to highlight it was the first vaccine available on the market.

In August 2020, the Russian government announced that they had developed a highly effective vaccine against COVID-19, Sputnik V. Despite many questions over its effectiveness and testing, it began to distribute globally.[75]

[73] Davis, Julia; "Russia, China Team Up to Peddle Insane U.S. COVID Lab Theory"; The Daily Beast; 9 April 2021; https://www.thedailybeast.com/russia-china-team-up-to-peddle-insane-us-covid-lab-theory.
[74] Dubow, Lucas, & Morris; 2021.
[75] Tetrault-Farber, Gabrielle and Vladimir Soldatkin; "Putin Hails New Sputnik Moment as Russia is First to Approve a COVID-19 Vaccine"; Reuters; 11 August 2020; https://www.reuters.com/article/us-health-coronavirus/russia-vaccine-put/putin-hails-new-sputnik-moment-as-russia-is-first-to-approve-a-covid-19-vaccine-idUSKCN25712U.

[76]

Simultaneously, via state media and online covert actors, Russians began actively attempting to denigrate and call into question Western-developed vaccines, including Pfizer, Moderna, AstraZeneca, and Johnson & Johnson. This included engaging with anti-vaccine activists, emphasizing conspiracy theories about Western-developed vaccines, and highlighting any setbacks in the various research efforts by the Western pharmaceutical companies.[77] As a result of this effort, at least initially, there were some regions where countries and populations grew more open to the Sputnik V vaccine, especially when there was no alternative, and the Russian state was offering to donate the vaccine to help.[78]

With time, however, as Western developed vaccines began to be released, Russian state media and covert actors became even more aggressive in attacking these vaccines, often targeting communities in the United States seemingly skeptical of vaccines. This included exploiting partisan divisions that developed within the United States over vaccines and encouraging even further divisions within the United States by targeting partisan organizations.[79] Additionally, in at least one documented instance, using private sector actors in Moscow, social media influencers in France and Germany were solicited to promote false narratives about

[76] Reuters (2021) Russia to supply first batch of Sputnik V vaccine to Philippines next month. Retrieved from https://www.reuters.com/business/healthcare-pharmaceuticals/russia-supply-first-batch-sputnik-v-vaccine-philippines-next-month-ifx-2021-03-19/.
[77] Dubow, Lucas, & Morris, 2021.
[78] Campbell, J. Russian Disinformation Popularizes Sputnik V Vaccine in Africa; Council on Foreign Relations; 10 December 2020; https://www.cfr.org/blog/russian-disinformation-popularizes-sputnik-v-vaccine-africa.
[79] Virality Project, 2022.

Pfizer.[80] [81] However, at the beginning of 2022, observers began to notice a shift in energy by Russian disinformation actors at the state level, as well as covertly, increasingly devoting energy to Russia's neighbor, Ukraine.

Russia's Disinformation Pivot to Ukraine

Historically, Russia has devoted significant energy to trying to influence the populace of the countries in its "near abroad," particularly those countries that were previously part of the Union of Soviet Socialist Republics (USSR). Since Ukraine's most recent revolution, the "Maidan Revolution," in February 2014, which ousted the pro-Russian President, Viktor Yanukovych, Russia has continuously exerted significant energy trying to prevent Ukraine from integrating completely with Western Europe. As part of this effort, various disinformation efforts emanating from Russia have targeted Ukraine and its Western allies, including the United States. Most recently, for example, before the 2020 U.S. Presidential election, the Treasury Department sanctioned a member of the Ukrainian Parliament for acting at the behest of the Russian government to promote false narratives regarding then-candidate Joe Biden as part of an effort to influence the presidential election[82]. However, Russia's decision to invade Ukraine in February 2022 further proved to be, even for Ukraine, a massive escalation in their effort to change Ukraine's political trajectory.

While it has only been five months since Russia further invaded Ukraine on February 24, there was an almost immediate change in disinformation narratives being tracked back to Russian or Russian-backed actors. Specifically, various individuals in the U.S. and Europe who had been actively trying to counter COVID-19 disinformation noticed that immediately following the war in Ukraine; they were suddenly not encountering the typical vitriol they faced on social media[83]. A separate report indicated that across Europe, fact-checkers noticed a significant change in the messaging they were witnessing on available channels on social media

[80] Dubow, Lucas, & Morris, 2021.
[81] Krutov, Mark, Sergei Dobrynin, Mike Eckel, and Carl Schreck; ”Exclusive: Meet the Murky Russian Network Behind an Anti-Pfizer Disinformation Drive in Europe” ; Radio Free Europe/Radio Liberty; 27 May 2021; https://www.rferl.org/a/russia-pfizer-covid-disinformation-serebryanskaya-murky-vaccine-influencers/31277170.html.
[82] U.S. Treasury Department; “Treasury Department Sanctions Russia-Linked Election Interference Actors”; U.S. Department of Treasury Press Release; 10 September 2020; https://home.treasury.gov/news/press-releases/sm1118.
[83] Schreiber, Melody; “‘Bot Holiday’: COVID Disinformation Down as Social Media Pivot to Ukraine”; The Guardian; 4 March 2022; https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

that had, for the past two years, been promoting false narratives and disinformation about COVID-19 and its vaccines.[84]

Starting almost as soon as the conflict erupted, fact-checkers in multiple European countries, including Denmark, France, Germany, Italy, Poland, and Spain, noticed a shift by actors promoting hoaxes and disinformation about COVID-19 towards addressing the conflict in Ukraine.[85] In contrast to the COVID-19 disinformation narratives that focused on fomenting fear and skepticism in public, the messaging surrounding the war in Ukraine focused on providing pro-Russian voices an audience, minimizing Russia's responsibility for the war, and presenting Russia's invasion as a legitimate operation.[86] While the medium used to promote the COVID-19 disinformation narratives varied, from Telegram channels to Facebook to news websites, the messages shifted from COVID-19 to defending Russia and promoting false reports about Ukraine, many of which reflected the Russian government's statements.[87] However, there were cases where actors promoting false narratives and disinformation regarding COVID-19 were not supportive of Russia's invasion of Ukraine, but such as in a case in Germany, they ended up losing significant support for their Telegram channel as a result.[88]

Whether disinformation actors will continue to focus on Ukraine remains to be seen. Still, individuals susceptible to hoaxes and false narratives about COVID-19 likely remain particularly vulnerable to disinformation on other matters, primarily if the messaging emanates from the same source. According to the Atlantic Council's Digital Forensic Research Lab, individuals who were already following these social media accounts or websites promoting hoaxes and disinformation regarding COVID-19 were primed to disbelieve the U.S. government's messaging surrounding the war in Ukraine.[89] The European Digital Media Observatory (EDMO) noted that there are likely various reasons for the shift from focusing on COVID-19 to the war in Ukraine, but among them was that the war became the primary news headline, so actors promoting

[84] Loguercio, Laura and Tommaso Canetta; "How COVID-19 Conspiracy Theorists Pivoted to Pro-Russian Hoaxes"; European Digital Media Observatory; 30 March 2022; https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/.
[85] Loguercio and Canetta, 2022.
[86] Loguercio and Canetta, 2022.
[87] Loguercio and Canetta, 2022.
[88] Loguercio and Canetta, 2022.
[89] Contreras, Brian & Wendy Lee; "Putin Targets Lots of Americans with Disinformation. One Example? Anti-vaccine Groups"; Los Angeles Times; 25 February 2022; https://www.latimes.com/business/technology/story/2022-02-25/heres-what-putins-disinformation-war-looks-like-on-the-internet.

disinformation needed to shift focus to keep the public's attention.[90] Some experts, however, argue the conspiracy theories surrounding COVID-19 remain out there and that these actors have chosen to shift focus for now and will return at some point.[91] However, at least one conspiracy theory has tried to meld the two issues, alleging the conflict in Ukraine was manufactured by the U.S. government to distract from the damage COVID-19 vaccines were causing.[92]

As noted earlier, China and Russia have often crossed paths in promoting disinformation narratives but diverged in their foci. In the case of the conflict in Ukraine, the Chinese government has made a concerted effort via public statements, state media, and social media actors to mirror Russian messaging regarding the war. In May 2022, the State Department's Global Engagement Center (GEC) outlined how the Chinese government had continuously echoed or amplified Russian disinformation regarding the conflict in Ukraine. First, by denying U.S. warnings about Russia's imminent invasion in February, and later, by amplifying Russia's disinformation narratives alleging the U.S.-sponsored biological weapons laboratories in Ukraine.[93] Since March, the Chinese government and state media have also regularly avoided reporting on atrocities committed by Russian forces in Ukraine, including bombings of civilian targets, and minimizing the U.S. and other Western reports about Russia's actions in Ukraine.[94] It remains unknown how long the conflict in Ukraine will go on. Still, many observers have also noted China's government has a vested interest in understanding how to counter the narratives Russia is facing as China's government addresses its alleged threats closer to home.

China's Disinformation Foci

In contrast to Russia's disinformation, which, as with COVID-19, has a variety of objectives and targets in the U.S. and other parts of the globe, China's disinformation narratives have primarily focused on protecting China's image and reinforcing the importance of China's

[90] Loguercio and Canetta, 2022.
[91] Schreiber, 2022.
[92] Contreras & Lee, 2022.
[93] State Department, "People's Republic of China Efforts to Amplify the Kremlin's Voice on Ukraine"; Global Engagement Center - State Department; 2 May 2022; https://www.state.gov/disarming-disinformation/prc-efforts-to-amplify-the-kremlins-voice-on-ukraine/.
[94] ibid.

national sovereignty.[95] In recent years, there has been an evolution in how China conducts disinformation operations, as seen with COVID-19. However, outside of COVID-19 disinformation and propaganda, China's efforts have traditionally focused on emphasizing China's national sovereignty, including over contested territory and activities in parts of China, including Xinjiang, Tibet, Hong Kong, and the legitimacy of China's claim to the island of Taiwan.[96] However, as with COVID-19 disinformation efforts, there has been an evolution in China's approach to disinformation, as well as to the goals of their disinformation efforts.

Historically, according to the Atlantic Council, China recognized the importance of being cautious when promoting propaganda and trying to influence foreign actors, as their government desired more significant investment from foreign businesses and to enhance relationships with foreign governments.[97] However, with the rise of President Xi and China's increased influence and capabilities on the world stage, there has been an increasingly aggressive effort by Chinese state media and government actors to project its influence globally, including through disinformation.

[98]

[95] Kalensky, Jakub; "Six Reasons the Kremlin Spreads Disinformation About the Coronavirus"; The Atlantic Council; 24 March 2020; https://www.atlanticcouncil.org/commentary/article/six-reasons-the-kremlin-spreads-disinformation-about-the-coronavirus/.
[96] Kalensky, 2020.
[97] Kalensky, 2020.
[98] Radio Free Asia (2020). China's Wolf Warrior Diplomats: Is Life Imitating Art? Retrieved from https://www.rfa.org/english/cartoons/china-wolf-warrior-cartoon-06012020163820.html.

The Alliance for Securing Democracy noted that China is presently trying to portray itself and its governmental system as a legitimate alternative to Western democratic governance.[99] Additionally, a core focus of China's disinformation efforts remains asserting China's sovereignty over the aforementioned areas of the country, as well as Taiwan. As a result of these dual foci, China is beginning to embrace a more aggressive approach to disinformation and broader malign influence.

According to the Digital Forensic Research Lab (DFRL), this increasingly aggressive approach has included embracing some of the tactics employed by Russia, such as increased engagement on social media platforms, including Facebook, Twitter, and YouTube.[100] However, foreign observers have noted that many of these efforts remain less effective than their Russian counterparts. On social media, while the Chinese government has become increasingly aggressive in promoting its narratives on everything from Taiwan to defending China's treatment of the Uyghurs, many of their initiatives have been easily identified by the social media companies and have been observed not to be nearly as influential.[101] Despite these challenges, many observers have noted the Chinese government is beginning to devote more significant resources to disinformation regarding COVID-19. While they may not have been successful yet, the concern may change, and their actions in Taiwan may indicate their broader approach to disinformation and malign influence efforts.

In 2020, Taiwan held Presidential elections and faced an onslaught of Chinese propaganda and disinformation initiatives. This included some heavy-handed tactics that were perceived to have backfired in that election; however, as the candidate perceived as "pro-Taiwan" was elected.[102] Since then, China has been behind efforts to promote false stories about nonexistent protests in Taiwan, false warnings that ballots for an opposition party would be invalidated and promoting false stories about pro-democracy advocates from Hong Kong that

---

[99] Solon, Olivia & Ken Dilation; "China's Influence Operations Offer a Glimpse into the Future of Information Warfare"; 21 October 2020; https://www.nbcnews.com/business/business-news/china-s-influence-operations-offer-glimpse-future-information-warfare-n1244065.

[100] Solon, Olivia & Ken Dilation; "China's Influence Operations Offer a Glimpse into the Future of Information Warfare"; 21 October 2020; https://www.nbcnews.com/business/business-news/china-s-influence-operations-offer-glimpse-future-information-warfare-n1244065.

[101] Kalensky, 2020.

[102] Zhong, Raymond; "Awash in Disinformation Before Vote, Taiwan Points Finger at China"; The New York Times; 6 January 2020; https://www.nytimes.com/2020/01/06/technology/taiwan-election-china-disinformation.html.

moved to Taiwan.[103] A Taiwanese think tank compared these efforts to the ultimate goal that Russia has tried to do in the U.S.: to crush people's confidence in the democratic system.[104] As part of this more nuanced effort, China has not only focused on direct influence on social media but also via Chinese and foreign actors to promote their pro-China messaging.

In 2021, multiple reports identified several "vloggers" from the U.S., Canada, and the U.K. promoting pro-China party lines in their videos. These "vloggers" all denied being influenced by the Chinese government. Still, some acknowledged they were receiving financial support to visit Chinese cities and regions, including Xinjiang, where international media has regularly reported on the Chinese government's maltreatment of its Uyghur population.[105,106] This has also included efforts by foreign language Chinese press, such as the China Global Television Network applying a lesson from Russia's state-sponsored media organization, R.T., and trying to hire foreign nationals to promote China's state messaging on CGTN.[107] Again, these influence efforts are reflective of a broader effort by the Chinese government to counter any criticism of the Chinese state by foreign actors and reflective of a different focus than Russia regarding its disinformation efforts.

When the new head of MI-5, Ken McCallum, entered office, he stated, "…if Russia's influence operations are like bad weather, China's growing operations are like climate change - far more destructive".[108] Much of China's influence efforts have focused on either countries close in proximity, such as Taiwan and the Philippines, or on matters directly relevant to the Chinese state to defend the integrity of the government. However, multiple researchers and analysts noted that various components of the Chinese government are increasingly devoting significant resources, both online and via diplomatic means, to push new disinformation narratives that directly impact citizens in the West. Additionally, the Chinese government had used its increasingly powerful economic clout to discourage foreign businesses from speaking out against the government, as was seen very publicly when an NBA coach released a personal statement

[103] Zhong, 2020.
[104] Zhong, 2020.
[105] Allen, Kerry & Sophie Williams; “The Foreigners in China’s Disinformation Drive”; BBC News; 11 July 2021; https://www.bbc.com/news/world-asia-china-57780023.
[106] Mozur, Paul, Raymond Zhong, Aaron Krolik, Aliza Aufrichtig and Nailah Morgan; ”How Beijing Influences the Influencers”; The New York Times; 13 December 2021; https://www.nytimes.com/interactive/2021/12/13/technology/china-propaganda-youtube-influencers.html.
[107] Allen and Williams, 2021.
[108] Solon & Dilation; 2020.

supporting protests in Hong Kong, and the NBA suddenly lost broadcast rights in China.[109] These types of responses, while not apparent disinformation, provide greater room for it as foreign news actors may be discouraged, for economic reasons, from criticizing an increasingly powerful economic actor that could damage their bottom line.

Private Sector Disinformation Targets

The private sector has been the target of mis-, dis-, and malinformation from a variety of sources ranging from state actors, the subject of this discussion, to other corporate actors, potentially part of the competitive process, and opportunistic actors such as the previously mentioned Bubble Yum example.[110] Their actions pose both threats and risks to the private sector.

[111]

Healthcare

Cyber operations in healthcare present different challenges and risks than in other industries, including those of other critical infrastructure sectors. In healthcare, these operations can directly impact patient safety, resulting in patient harm, including death. In addition to stolen healthcare data being used for numerous criminal purposes, the large and ever-growing volume

[109] Kalensky, 2020.
[110] Wardle, C. (2020) Understanding the Information Disorder. FirstDraft. Retrieved from https://firstdraftnews.org/long-form-article/understanding-information-disorder/.
[111] Wardle, 2020.

of connected medical devices and systems pose a significant risk to patient safety if not protected.[112] A significant cyberattack scenario on a hospital, pharmaceutical company, or other healthcare organization could result in a loss of availability of their services or products or the confidentiality of patient data, and a lack of trust in these healthcare entities.

[113]

Foreign cybercriminals and nation-state affiliated adversaries have long targeted the US healthcare and public health sector. Despite having the capability to weaponize their cyber capabilities against US critical infrastructure, neither Russia nor China has launched large scale attacks against any of the US critical infrastructure sectors, including healthcare, since the Russian invasion of Ukraine.[114] However, the Russian military intelligence agency and other Russian government or Russian affiliated organizations have continued to launch smaller, less complex attacks including sustained DDoS attacks against Ukrainian government websites and infrastructure.[115] Healthcare data breach reports that showed a marked decrease from December 2021-March 2022 have risen steadily since to near record numbers.[116]

The lines between cyber criminals and intelligence operations in, amongst others, Russia and China, have increasingly blurred. This overlap adds more complexity to the challenges of

[112] Health Care Industry Cybersecurity Task Force—Report on Improving Cybersecurity in the Health Care Industry, June 2017. Retrieved June 21, 2022 from https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.
[113] Silva, A. (2020) Ransomware Attacks Against Hospitals on the Rise. Microwiz Technology. Retrieved from https://microwize.com/ransomware-attacks-against-hospitals-on-the-rise/.
[114] Wolff, J. (2022, March 2). Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine. Time. Retrieved July 8, 2022 from https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/.
[115] Fendorf, Kyle and Miller, Jessie. (2022, March 24). Tracking Cyber Operations and Actors in the Russia-Ukraine War. Retried July 18, 2022 from https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.
[116] HIPAA Journal/ 2022 Healthcare Data Breach Report-HIPAA Journal (2022, June 21). Retrieved July 6, 2022, from https://www.hipaajournal.com/may-2022-healthcare-data-breach-report/.

analyzing and attributing cyberattacks in real-time. In some cases, these groups are assisted by intelligence services. The recent Russian invasion of Ukraine increased cyberattacks for cybercrime and espionage purposes against US critical infrastructure sectors, including healthcare, by the Russian state and Russian-sponsored actors. These cybercriminals continue to evolve their ransomware and other attack methods in the wake of new protection tactics by industry and government.[117]

According to the HHS Cybersecurity Program Office of Information Security, there are three potential threat groups related to the Russia-Ukraine conflict: Belarussian government organizations, cybercriminal groups based out of Russia and neighboring states, and Russian government organizations.[118] Russian-affiliated cybercrime organization Conti is considered one of the most successful and ruthless Russian ransomware groups, although their attacks are not limited to ransomware. Despite promising not to attack healthcare organizations during the pandemic, Conti has launched cyberattacks against healthcare organizations in the United States and several other countries over the past two years.[119]

[117] Uberti, D. (2022, June 1) Line Between Criminal Hackers and Nation-State Threats Blurs, U.S. Officials Say. Wall Street Journal. Retrieved July 8, 2022 from https://www.wsj.com/articles/line-between-criminal-hackers-and-nation-state-threats-blurs-u-s-officials-say-11654109885.
[118] HHS Cybersecurity Program Office of Information Security (2022, March 1). The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector HHS HC3 Analyst Note March 1, 2022. Retrieved June 24, 2002 from https://www.hhs.gov/sites/default/files/russia-ukraine-cyber-conflict-analyst-note-tlpwhite.pdf.
[119] CISA (2022, May 9) Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, May 9, 2022. Retrieved June 18, 2022 from https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

[120]

During the first four months of 2022, Conti claimed responsibility for hacking healthcare organizations throughout the healthcare and public health sector, including an online prescription service, a biomedical testing facility, a surgery center, a cancer testing laboratory and a pharmaceutical company.[121] Directly following the Russian invasion of Ukraine, Conti announced their direct support for Russia and indicated they would target the critical infrastructure of nations attempting to thwart Russia's military actions.[122]

Like Russia, China has state-sponsored hacking groups that regularly attack US private and public entities, including critical infrastructure. Several attacks have resulted in confirmed system compromises, including US pipeline infrastructure.[123] Numerous security researchers have identified APT41 as a prolific Chinese state-sponsored cyberthreat group" responsible for significant numbers of cyberattacks against the United States.[124]

---

[120] Prewitt, J. (2021) Ireland's health care system was attacked on Friday by Conti ransomware. RoundNews. Retrieved from https://www.roundnews.com/world/europe/62592-irelands-health-care-system-was-attacked-on-friday-by-conti-ransomware.html.

[121] Krebs, Brian. (2022, April 18). Conti's Ransomware Toll on the Healthcare Industry. Retrieved July 4, 2022 from https://krebsonsecurity.com/2022/04/contis-ransomware-toll-on-the-healthcare-industry/.

[122] Bing, Christopher. (2022, February 25). Russia-based Ransomware Group Conti Issues Warning to Kremlin Foes. Reuters. Retrieved July 18, 2022 from https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/.

[123] CISA (2021, July 21) Alert (AA21-201A) Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013. Retrieved July 18, 2022 from https://www.cisa.gov/uscert/ncas/alerts/aa21-201a.

[124] Kharpal, Arjun (2022, March 9). China state-backed hackers compromised networks of at least 6 U.S. state governments, research finds. CNBC. Retrieved July 18, 2022 from https://www.cnbc.com/2022/03/09/china-state-backed-hackers-compromised-6-us-state-governments-report.html.

125

A joint advisory issued in June 2022 by the National Security Agency (NSA), the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) detailed a sustained operation focused on the exploitation of networking devices across large numbers of private and public sector entities.[126] In addition, in July 2022 the heads of the FBI and Britain's domestic security service MI5 urged industry leaders not to underestimate the sophistication and scale of China's campaign aimed at stealing intellectual property from Western technology companies.[127] As part of the Made in China 2025 plan mentioned, China is aggressively pursuing economic dominance and using this as a rulebook for the modern and innovative technology companies Chinese hackers target.[128]

[125] Paganini, P. (2020) APT41 actors charged for attacks on more than 100 victims globally. Security Affairs. Retrieved from https://securityaffairs.co/wordpress/108381/apt/apt41-doj-indictments.html.
[126] CISA (2022, June 10) Alert (AA22-158A) People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices. Retrieved July 18, 2022 from https://www.cisa.gov/uscert/ncas/alerts/aa22-158a.
[127] Colchester, Max. (2022, July 6). Heads of FBI, MI5 Issue Joint Warning on Chinese Spying. Wall Street Journal. Retrieved July 15, 2022 from https://www.wsj.com/articles/heads-of-fbi-mi5-issue-joint-warning-on-chinese-spying-11657123280.
[128] Lyngaas, Sean (2022, May 4). Chinese hackers cast wide net for trade secrets in US, Europe and Asia, researchers say. CNN. Retrieved July 19, 2022 from https://www.cnn.com/2022/05/04/politics/china-hackers-economic-espionage-manufacturing/index.html.

While reconnaissance against U.S. and other western critical infrastructure sectors has been ongoing throughout 2022, Russia, China and their affiliated entities have not launched large scale attacks against western critical infrastructure.[129] There are many theories as to why Russia has been either reticent or unable to launch large-scale attacks against the US or other western infrastructure as a supplement to kinetic war activities or as a response to western sanctions. Questions exist as to whether Russia has additional reserve cyber capabilities available, if Russia has neglected the development of more effective, more expensive cyber weapons, or if they lack adequate human and technical resources to launch sophisticated attacks.[130] However, the lack of action by Russia should not be perceived as a lack of capability.

Traditional Financial Sector Attack Vectors

Cyber threat actors frequently target the financial sector through traditional tactics, techniques, and procedures (TTPs) such as ransomware attacks, supply chain compromise, and malware infection.[131] The goal for these types of operations is to obtain maximum revenue and maximum impact on the target organization. One of the most effective vectors leveraged for monetary gain is ransomware.


132

[129] Kolbe, P., Morrow, M., & Zabierek, L.. (2022, February 24). The Cybersecurity Risk of an Escalating Russia-Ukraine Conflict. Harvard Business Review. Retrieved July 14, 2022 from https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict.
[130] Wolff, 2022
[131] Flashpoint Team. (2022, May 17). *Top 7 cyber threats to the Financial Services Sector in 2022*. Flashpoint. Retrieved July 21, 2022, from https://flashpoint.io/blog/top-7-cyber-threats-to-financial-services-sector-2022/
[132] Egan, M. (2016) NYSE Receives Credible Cyber Threat Against Website. Fox Business. Retrieved from https://www.foxbusiness.com/features/nyse-receives-credible-cyber-threat-against-website.

Threat actors capture stolen data and hold the information for ransom, often putting an organization and its customers at financial risk. Other traditional tactics used to target the financial industry are malware, e-skimmers, and formjacking. These attack vectors exploit various payment platforms and processes to obtain highly sensitive data such as PII (personally identifiable information) and credit/debit card information.[133] Recently, the financial sector has observed an uptick in threat actors leveraging synthetic identity fraud to commit financial crimes.[134] Synthetic identity fraud, a tactic in which criminals steal real PII and combine it with fake PII to open fraudulent banking accounts, is reportedly costing the financial industry an estimated $6 billion USD annually.[135] The financial sector has crafted security protocols to protect its systems and customers against traditional attack vectors; therefore, these malicious actors have adapted to other forms of financial exploitation. One of the newest tactics used to target executives with disinformation is to conduct fraud, extortion, and stock manipulation operations. [136]

Disinformation Targeting the Financial Sector

The financial sector is notably more resilient to disinformation campaigns than other critical infrastructure sectors such as healthcare and communications. Rather than targeting a global financial system or mature financial market, disinformation campaigns often target individuals to cause a business-wide impact.[137] Large-scale disinformation campaigns targeting a financial entity become slightly more effective when disinformation is spread among pre-

[133] Flashpoint, 2022.
[134] McKay, R. (2021, May 18). *Council post: The $6B synthetic identity fraud problem and assessing customer identity*. Forbes. Retrieved July 21, 2022, from https://www.forbes.com/sites/forbestechcouncil/2021/05/18/the-6b-synthetic-identity-fraud-problem-and-assessing-customer-identity/?sh=2f77e07f253b
[135] McKay, R. (2021, May 18). Council post: The $6B synthetic identity fraud problem and assessing customer identity. Forbes. Retrieved July 21, 2022, from https://www.forbes.com/sites/forbestechcouncil/2021/05/18/the-6b-synthetic-identity-fraud-problem-and-assessing-customer-identity/?sh=2f77e07f253b
[136] Bateman, J. (2020, July 8). Deepfakes and Synthetic Media in the financial system: Assessing threat scenarios. Carnegie Endowment for International Peace. Retrieved July 15, 2022, from https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.
[137] Bateman, J. (2020, July 8). Deepfakes and Synthetic Media in the financial system: Assessing threat scenarios. Carnegie Endowment for International Peace. Retrieved July 15, 2022, from https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.

existing negative news regarding the entity, further expelling a malicious narrative.[138] Synthetic media has proven to be the most effective form of disinformation capable of threatening market stability and is often leveraged to conduct fraud, extortion, and stock manipulation operations. Notably, the SEC deemed market manipulation illegal, yet only recently issued a bulletin flagging mis/disinformation spreading on social media with the ability to juice or depress individual stocks in 2015.[139] These operations rarely impact macroeconomics, yet they can potentially impact vulnerable developing countries experiencing financial crises.[140]

Social media users unknowingly sharing misinformation alone has significantly impacted the economy. For example, research conducted by the Economic Policy Institute and Forbes in 2018 showed financial advisors supplying false and misleading information cost the U.S. at least USD 17B.[141] Additionally, the American Institute of CPAs noted three in five Americans reported the spread of financial misinformation makes it more challenging to make critical financial institutions.[142] While misinformation is often challenging to identify without proper vetting, disinformation is deliberately deceptive. A common form of financial disinformation is crafting and sharing falsified financial trends. Arguably, social media provides a platform where users can share information to ensure market transparency and efficiency; however, malicious actors have weaponized social media to compromise market integrity and financial stability through financial disinformation.[143]

---

[138] Biancotti, C. & Ciocca, P. (2021, November 2). Financial Markets and social media: Lessons from information security. Carnegie Endowment for International Peace. Retrieved July 15, 2022, from https://carnegieendowment.org/2021/11/02/financial-markets-and-social-media-lessons-from-information-security-pub-85686.

[139] Lipsky, J., & Wechsler, W. (2021, February 1). Opinion: The game stop saga is a road map for the Kremlin and other enemies of America -- here's why. MarketWatch. Retrieved July 15, 2022, from https://www.marketwatch.com/story/the-gamestop-saga-is-a-road-map-for-the-kremlin-and-other-enemies-of-america-heres-why-11612208909?mod=mw_latestnews.

[140] Bateman, J. (2020, July 8). Deepfakes and Synthetic Media in the financial system: Assessing threat scenarios. Carnegie Endowment for International Peace. Retrieved July 15, 2022, from https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.

[141] Carson, R. (2018, October 14). Retirement savers are losing $17 billion a year from fake news and conflicts of interest. Forbes. Retrieved July 15, 2022, from https://www.forbes.com/sites/rcarson/2018/10/14/retirement-savers-are-losing-17-billion-a-year-from-fake-news-bad-advice-conflicts-of-interest/?sh=9854f32bec7c#5e635549bec74.

[142] AICPA. (2017) Fake financial news is a real threat to majority of Americans: New aicpa survey. Retrieved July 15, 2022, from https://us.aicpa.org/press/pressreleases/2017/fake-financial-news-is-a-real-threat-to-majority-of-americans-new-aicpa-survey.

[143] Biancotti and Ciocca, 2021

The Polish Experience with Disinformation [144]

145

In the period preceding the armed assault on Ukraine and from the beginning of the war, Russia intensified its use of active measures, including disinformation and cyberattacks against European countries, with particular emphasis on former Eastern Bloc countries. In the case of Poland, government institutions, critical infrastructure enterprises, and private companies were attacked. Among other things, government I.T. systems were attacked. For almost two weeks, the website of the Polish Air Rescue was down due to a ransomware attack. Since mid-February, Poland has had Charlie – the third (of four) – alert level concerning threats in cyberspace. The Digital Policy Promotion Department of the Prime Minister's Office reported an increase in the frequency of DDOS attacks targeting Polish institutions and national entities, which may cause difficulties in accessing services provided via the Internet.

In early 2022, Israeli firm Check Point Research reported a surge in cyber-attacks 2021. The increase in the number of attacks on government institutions was particularly felt in Poland – compared to the previous year; it was as high as 73 percent, indicates Interia and the Kosciuszko Institute, organizer of the CYBERSEC FORUM/EXPO event. They remind us that one of the attacks on government websites, which was thwarted, was carried out during the visit of President Biden to Poland. Russian and Belarusian hackers attacked Polish military email accounts through phishing attacks. The same hacking group (UNC1151) conducted cyberattacks on the email accounts of Polish politicians in 2020 as part of the hacking operation

[144] Contribution from Kacper Gradon, Ph.D. Honorary Visiting Fellow University College London. Fulbright Scholar and visiting scholar, University of Colorado Boulder. 2022.
[145] Ministry of Foreign Affairs (2020) Republic of Poland. Retrieved from https://www.gov.pl/web/diplomacy/eu-imposes-further-sanctions-aimed-at-combatting-cyber-attacks

"Ghostwriter," which focused on creating divisions within the ruling coalition in Poland and Polish society.

The "The Lazarus" hacking group is responsible for cyber-attacks against arms contractors worldwide. Their targets included entities from Poland and Ukraine. ESET specialists investigated the APT group "Lazarus," which carried out cyber-attacks on arms contractors worldwide, including in Poland; their actions were based on fake recruitment campaigns conducted on well-known websites and applications, e.g., LinkedIn and WhatsApp. According to the Polish Financial Supervision Authority, Polish financial institutions have come under a veritable cyber storm; today, the average Polish banking and finance company is attacked nearly a thousand times a week. The number of disinformation attacks has increased tremendously. Already on March 3, 2022, The Institute for the Study of Internet and social media informed that in the previous 24 hours, they identified – in Polish social media – over 120.000 cases of disinformation (a 20% increase) related to the War in Ukraine. The Institute identified the vast majority of these cases as anti- Ukrainian refugees oriented and pro-Russian and – most importantly – utilizing channels and accounts "formerly" associated with anti-Covid19-vaccination disinformation.

It looks like the anti-vaccine disinformation disappeared overnight and was replaced by anti-Ukraine and pro-Kremlin narratives. Russia is also pushing anti-refugee rhetoric in the health context (such as that Ukrainian refugees will strain our health system and bring diseases long eradicated in this part of Europe). Russian disinformation is intensifying the narrative that Poland should invade and occupy western Ukraine (actually, historically, these are Polish lands, but Poland has no territorial claims to them). Anti-refugee narratives are promoted, and Polish authorities and fact-checking NGOs are constantly debunking these.

Sanctions Against Russia

At the onset of the invasion of Ukraine, the United States and its European allies began imposing far-reaching sanctions against Russia. The sanctions targeted Russia’s financial and

energy sectors and individuals close to Vladimir Putin.[146] The sanctions were intended to pressure Putin to end the invasion and withdraw from Ukraine.[147]

148

The results have been mixed with past sanctions regimes against other countries. Through mid-July 2022, while the Russian economy is estimated to have contracted 10-15%, it has not ceased military operations in Ukraine.[149] Additionally, while European countries have greatly scaled back imports of Russian energy, China and India have greatly increased Russian energy imports, with China doubling its imports for the quarter ending in May and India increasing imports five-fold.[150]

There should be concerns that Russia, and perhaps China, may launch information campaigns in retaliation against the Ukraine-related sanctions. Disinformation, information intended to cause harm, may be used against Western companies regardless of whether they supported the sanctions regimes. Russia has a history of exploiting divides irrespective of whether a side of the narrative supports its position. The objective is to create controversy.[151]

---

[146] BBC News (2022). What are the sanctions on Russia and are they hurting its economy? Retrieved from https://www.bbc.com/news/world-europe-60125659.
[147] Wong, E. and Crowley, M. (2022) With Sanctions, U.S. and Europe Aim to Punish Putin and Fuel Russian Unrest. The New York Times. Retrieved from https://www.nytimes.com/2022/03/04/us/politics/russia-sanctions-ukraine.html?searchResultPosition=8.
[148] The Millennium Report (2017) EU Bashes US For New Sanctions On Russia; Germany Issues Threats. Retrieved from http://themillenniumreport.com/2017/07/eu-bashes-us-for-new-sanctions-on-russia-germany-issues-threats/.
[149] National Public Radio (NPR) (2022) Breaking down the effectiveness of the latest sanctions on Russia. Retrieved from https://www.npr.org/2022/06/06/1103270266/breaking-down-the-effectiveness-of-the-latest-sanctions-on-russia.
[150] Murtaugh, D. and Chakraborty, D. (2022) Russia pockets $24bn from selling energy to China, India. Aljazeera. Retrieved from https://www.aljazeera.com/economy/2022/7/6/russia-pockets-24b-from-selling-energy-to-china-india.
[151] Moy & Gradon, 2020.

Information campaigns do not necessarily have to be made of false information or intended to cause unjustified harm. In 2013, Gabriela Cowperthwaite premiered a documentary film Blackfish, depicting SeaWorld's treatment of killer whales in captivity resulting in the resignation of the chief executive officer, a steep decline in the corporation's market value, and an investigation into safety practices.[152]

In addition to government-imposed sanctions, numerous private sector companies have exited Russia or curtailed nearly all their operations there. Private sector companies have varied in supporting the sanctions regimes against Russia. Responses have ranged from closing operations and exiting Russia to other companies continuing to conduct business as usual. As of late-June 2022, 326 either halted their operations in Russia or exited completely, and 474 curtailed most or nearly all of their operations but kept their operations open for a return to Russia.[153] On the A list, there were 93 Industrial companies like consulting, transportation and manufacturing. Consumer Staples and Discretionary were 75, including cruise lines, Heineken, and fast-food firms.

Disinformation related to business organizations and their products is not new. In 1977, a false rumor began spreading that the secret ingredient in Lifesaver Brand's Bubble Yum was spider eggs causing sales to plummet despite attempts to dispel the misinformation.[154] At the time, this was labeled *urban legend* rather than disinformation or misinformation. Conspiracy theories range from the moon landings being faked to HIV/AIDS being developed in a U.S. Army laboratory to wipe out homosexuals and Black people.[155] The HIV/AIDS theory may be attributable in whole or in part to the Soviet disinformation campaign *Operation Infektion,* aspects of which continue to circulate.[156]

Notably, some vulnerabilities to disinformation may result from actual corporate actions. During the 1970s, ExxonMobil and other petroleum-related companies advanced narratives

---

[152] Rice, C. & Zegart, A. (2018) Political Risk: *How Businesses and Organizations Can Anticipate Global Insecurity*. Twelve Hachette Book Group. New York, NY.
[153] Yale School of Management (2022) *Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain*. Retrieved from https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain.
[154] Hunter, A. (2016) Bubble Yum, Spider Eggs and Leonardo DiCaprio. The Weekly Voice. Retrieved from http://weeklyview.net/2016/09/15/bubble-yum-spider-eggs-and-leonardo-dicaprio/.
[155] Time (2009) *Conspiracy Theories*. Retrieved from https://content.time.com/time/specials/packages/completelist/0,29569,1860871,00.html.
[156] Boghardt, T. (2009) Soviet Bloc Intelligence and Its AIDS Disinformation Campaign. *Studies in Intelligence* 53(4) (2009).

denying climate change despite evidence in their possession from their scientists.[157] During the 1960s, tobacco companies disseminated significant disinformation denying the health risks associated with their products.[158] The truthfulness or lack of truthfulness of a narrative directed against a corporation is not essential for conducting a disinformation campaign. It is vital to remember that the objective is to cause disruption.[159]

Russian and Chinese state-controlled media, including Sputnik, RT, and CGTN, are often cited as essential sources of state-sponsored disinformation. Russian news outlets seem to follow a pattern in which 80% of the information they report is accurate, and a much smaller percentage is disinformation. It is important to remember that accurate information can play a significant role in a disinformation campaign. For example, a late-June RT article on Microsoft exiting Russia seemed very factual and nonjudgmental and noted that Apple, IBM, SAP, Cisco, and Dell were also curtailing operations.[160]

Conclusions

Russia and China exemplify contrasting national objectives that can be served through malign influence campaigns. Russia perceives Western democracies and institutions as their greatest threat and seeks to undermine and discredit them. In contrast, China aims to be the preeminent power in Asia in the near term and, in the longer term, lead the world in economic, military, and political power. Traditional intelligence operations are often used to increase influence, undermine Western alliances, and attack the United States, creating internal discord and influencing internal decision-making. Russia uses intelligence agencies, surrogates, and a wide-ranging set of tools in this effort. An evolving tactic in today's media landscape is disinformation to spread conspiracy theories attempting to cause discord. For example, *Operation Infektion* is a tenacious conspiracy theory that continues to apply today, particularly

[157] Powell, A. (2021) Tracing Big Oil's PR war to delay action on climate change. *Harvard Gazette*. Retrieved from https://news.harvard.edu/gazette/story/2021/09/oil-companies-discourage-climate-action-study-says/.
[158] McKee, M. (2017) Big Tobacco: The Pioneer of Fake News. *Journal of Public Health Research* 6(1). DOI: 10.4081/jphr.2017.878.
[159] ODNI, 2022.
[160] RT (2022) US tech giant pledges to leave Russia. Retrieved from https://www.rt.com/business/557706-microsoft-leaving-russia-sanctions/.

over the Internet in social media. Russia's disinformation efforts related to COVID-19 were varied, employing a variety of narratives and conspiracy theories and tailoring their messaging to multiple groups. Chinese disinformation and propaganda efforts were, on the whole, unified and supported its overall state strategy. Russia has a history of exploiting divides regardless of whether a side of the narrative supports its position. Disinformation, information intended to cause harm, may be used against Western companies irrespective of whether they supported the sanctions regimes.

China regularly leverages disinformation to conduct influence operations to extend its power globally and displace the United States as the most influential country. Additionally, China uses a network of media organizations to disseminate misinformation online at home and abroad. It produces misleading information on U.S.U.S. issues, including election voter fraud and COVID-19, and echoes QAnon conspiracy theories. For example, during the COVID-19 pandemic, China was the leader in spreading disinformation about the origin of the disease, in part, against then-President Donald Trump's labeling the coronavirus condition. Chinese government-linked disinformation efforts worked to obfuscate the virus's origins, evoking multiple conspiracy theories including that the virus originated in the United States or one of its international laboratories. Frequently, China's messaging focused on protecting the country's image by calling into question the origins of COVID-19 and highlighting the government's response to it.

Additionally, in 2021, multiple reports identified several vloggers from the U.S., Canada, and the U.K.U.K. promoting pro-China party lines in their videos. These vloggers denied being influenced by the Chinese government, yet, some acknowledged they were receiving financial support. Financed by the Chinese government, they visited Chinese cities and regions, including Xinjiang, where international media has regularly reported on the Chinese government's maltreatment of the Uyghur population.

Disinformation influences governments and their populations and impacts critical sectors, including financial services and healthcare. The financial sector seems more resilient to disinformation campaigns than other sectors such as healthcare and communications. Resilience likely varies by industry and needs to be explored further. Rather than targeting a global financial system or mature financial market, disinformation campaigns often target individuals to cause a business-wide impact. Large-scale disinformation campaigns targeting a financial entity become

slightly more effective when disinformation is spread among pre-existing negative news regarding the entity, further expanding a malicious narrative. A recent study conducted jointly by the Economic Policy Institute and Forbes magazine in 2018 showed false and misleading information costing the United States at least $17 billion. Foreign cybercriminals and nation-state affiliated adversaries have long targeted the U.S.U.S. healthcare and public health sector. Despite having the capability to weaponize their cyber abilities against U.S.U.S. commercial sectors, neither Russia nor China has launched large-scale attacks against any U.S.U.S. critical infrastructure sectors, including healthcare, since the Russian invasion of Ukraine. There are many theories as to why Russia has been either reticent or unable to launch large-scale attacks against the U.S.U.S. or other western infrastructure as a supplement to kinetic war activities or as a response to western sanctions. Questions exist as to whether Russia has additional reserve cyber capabilities available, if Russia has neglected the development of more effective, more expensive cyber weapons, or if they lack adequate human and technical resources to launch sophisticated attacks.