3

From Free Speech to False Speech

Analyzing Foreign Online Disinformation Campaigns Targeting Democracies

Rachel Brooks-Bitterli

INTRODUCTION

Popular technology platforms enable users to create an account, sometimes anonymously or with minimal identity verification. Users can post and share content instantaneously to networks online. As this user-generated content is available immediately and not fact-checked first, social media is ripe for manipulation from disinformation. By the time disinformation campaigns are detected, they may have propagated rampant misinformation – unintentionally false information – as real users share untrue content they see and believe to be accurate with their networks.

Online disinformation efforts pose challenges for detection and mitigation. Technology companies, governments, and civil society struggle to promptly and adequately respond to ongoing threats to the information environment. Governments can be disinformation campaigns' culprits within their own countries; look no further than *New York Times* reports of US President Donald Trump's disinformation-perpetuating commentary on mail-in voting leading up to the 2020 election (Sanger & Kanno-Youngs, 2020; Stolberg & Weiland, 2020). However, this chapter's scope focuses on Russian and Chinese campaigns rather than within-country campaigns.

Disinformation campaigns can drive people to reinforce confirmation biases and spread fabricated information they believe is accurate. Today's vast online information environment bombards users with headlines and makes it challenging to discern trustworthiness. This information overload can benefit education and knowledge accessibility. However, it also allows actors to manipulate social media for their agendas.

This chapter investigates the extent to which Russian and Chinese online disinformation campaigns attempt to influence democracies to further their strategic aims. It is vital to first locate the challenge of disinformation within the international security landscape and today's "post-truth" world. While disinformation – intentionally false information – is not new, the internet presents unique challenges in detecting, responding to, and curbing such content.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

States can exploit this environment by using social media's algorithms and capabilities to spread disinformation. Bots and other technologies offer cheap, scalable, automated ways to amplify coordinated campaigns. These efforts intentionally center on existing societal divides in the targeted countries. Such divisions include the climate crisis, racial strife, and democratic processes. The latter is this study's focus.

Research Questions and Methodology

This research discusses the extent and how Moscow and Beijing employ online disinformation campaigns to exploit the vulnerabilities of democracies and advance strategic aims. At the heart of this research is an assessment of the chief similarities and differences in tactics identified through dyads between Russia, China, and specific democracies.

The methodology employs a review of public reports, archives, and news content coupled with contextualized case studies. This approach centers on Russia and China as the primary propagators of online disinformation against democracies. We focus on well-researched, major democracies to achieve a global perspective of countries affected, although we acknowledge there are other, often less-studied examples, including democracies in developing countries. Each case study incorporates varying examples of global disinformation attacks credibly attributed to originating countries.

Limitations

Limitations stem from the difficulty of studying something inherently involving deception. The internet's ability to provide anonymity presents challenges in identifying disinformation's exact origin and extent. Aspects of social networks can obfuscate whether untrue content is ill-informed misinformation or deliberate disinformation. This work focuses on coordinated, professionalized examples of disinformation against democracies attributed to authoritarian states. Many authoritarian states' aims remain covert; thus, we look to history, current events, and scholarly experts to analyze authoritarian goals when official statements are unavailable. Another challenge to disinformation is accurately measuring reach and impact, including the outcomes of a disinformation-heavy article or tweet on voter preferences. Confounding factors influence users' views; therefore, we look to available social media data for best estimations.

DEMOCRACY AND AUTHORITARIAN THREAT

Inherent in the research is the belief democracies need to increase their resilience against foreign governments' efforts to exert influence through disinformation and acknowledgment of disinformation's complexity and international prevalence. Disinformation is not one-sided from authoritarian regimes to democracies but can also emerge within democracies, including sometimes targeting authoritarian

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

states. We also recognize differences between stable, established democracies and emerging, vulnerable, or crisis-ridden democracies.

Russia and China present two intriguing case studies of authoritarian regimes deploying disinformation against democracies for multiple reasons. Russia's President Vladimir Putin and China's President Xi share a rapport engendering security cooperation and "remarkably frequent" engagements supporting a "growing agreement about how the world should be" (Kendall-Taylor & Shullman, 2018, p. 1). They share an understanding that eroding democracy will contribute to their mutual aims, including weakened Western power. Later sections present core similarities and differences between known Russian and Chinese disinformation campaign strategies aimed at democracies.

Many influence operations are at least partially covert, notably aided by the internet's potential for anonymity and globalization (U.S. Department of Homeland Security, 2020; Wray, 2020). A frequent tactic of influence operations is adversaries creating artificial personas and fabricated narratives to denigrate democratic institutions (Wray, 2020). Despite most disinformation's covert nature, reputable sources, such as official government documents, international institutions, and fact-checked nonpartisan media, linked examples discussed to the Russian or Chinese government. While this research focuses on governments' foreign influence campaigns, non-state actors are also responsible for initiating disinformation campaigns. Including non-state operations would become unwieldy; thus, we remain focused on efforts judged to be launched, backed, or otherwise supported by governments.

Definitions: Misinformation and Disinformation

While disinformation and misinformation are both dangerous and deepen societal divides, the critical difference is intent. This research is concerned with disinformation – sharing false information in intentional efforts to harm or deceive. Misinformation is the "spreading of unintentionally false information" (Theohary, 2018, p. 5). Misinformation can manifest as internet users sharing hoaxes or conspiracy theories they believe are authentic.

Typical examples of disinformation include doctored photos, inaccurate news articles, or tampered official documents purposely planted online. These instances occur within the information environment, which encompasses systems and actors "collect[ing], disseminat[ing], or act[ing] on information" (Theohary, 2018, p. 5). Disinformation in international relations is a pervasive challenge, especially given the internet's potential for anonymity, low entry cost, and global spread.

Analyzing Online Disinformation from Russia and China

Russia and China are two powers seeking to challenge or undermine norms they view as dominated by the West. Where publications sometimes focus on one or the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

other, this research analyzes their distinct aims side by side in deploying disinformation against democracies. While there is ample research on historical disinformation from the Soviet Union during the Cold War and its aftermath, renewing this study after Putin's presidency began in 2000 is helpful. Likewise, President Xi rose to power in China in 2012 and implemented bold breaches of international norms and law, including cyberattacks (White House, 2015). Coupled with China's economic and geostrategic power, these influence campaigns make valuable case studies.

Despite authoritarian similarities between Russian and Chinese disinformation targets and strategies, there are distinct contrasts. One difference is Russia's long-standing tradition of implementing international disinformation campaigns that precede the internet's advent. In comparison, China's power and participation in the global disinformation landscape have grown in recent years (Bradshaw & Howard, 2019; Wray, 2020). This chapter creates an analytical framework to map authoritarian regimes' foreign influence efforts against democracies: (1) through longer-term, ambient disinformation, (2) during transitions of political power, and (3) during social and cultural divides. This framework drives our analysis.

RUSSIAN ONLINE DISINFORMATION CAMPAIGNS TARGETING DEMOCRACIES

Russian Disinformation's Strategic Aims

Moscow's aims and global positioning as an authoritarian geostrategic power help us contextualize Russian disinformation. Because Russian disinformation provides some of the most well-known and credibly attributed examples of foreign interference, Kalathil (2020, p. 36) suggests the Russian state serves as a "model for other authoritarians' efforts." Evidence of Russian online disinformation affecting democracies across Europe, North America, and elsewhere confirms the reach of Kremlin-initiated interference campaigns.

Bernstein (2011) calls Russia a "'hybrid' authoritarian regime" under Presidents Putin and Medvedev because of the existence of some democratic institutions, including multiparty elections and competitive parties. These democratic institutions are restricted yet noteworthy. In theory, these institutions' existence should indicate that democracy's norms are accepted and a possibility – if meager under Putin's regime – of movement toward a more complete democracy.

Russia's strategy has long incorporated influence operations, with the Kremlin-supported Internet Research Agency (IRA) beginning as an effort to exert influence within Russia (Pomerantsev, 2019). Turning to Russia's foreign targets, this research concentrates on two categories: geographically close democracies and Western democracies. Russia deployed strategic efforts externally with post-Soviet "near abroad" targets of Estonia, Georgia, Latvia, Moldova, Lithuania, and especially Ukraine (Kalathil, 2020; Sukhankin, 2019). Because Russia assesses its might

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

compared to the United States and other powers, the Kremlin also targeted Western democracies. Weakened democracy, particularly in the West, helps increase Russia's perception of its power and influence.

Kendall-Taylor and Shullman (2018) describe Russia's global strategy as "confrontational and brazen." The Kremlin's assault on democratic institutions spans foreign interference in elections, disinformation campaigns, and corruption to erode global commitment to democracy. This research focuses on the disinformation component while recognizing disinformation as one method within the broader Russian foreign influence approach. Even within disinformation, multiple strands of influence emerge. While some understand disinformation as only overt falsehoods, this work asserts that disinformation is a complex challenge for democracies, including tactics such as the Russian military intelligence (GRU) use of narrative or information laundering and boosterism, as supported by DiResta and Grossman (2019). Narrative laundering is when "a story is planted or created and then legitimized through repetition or a citation chain across other media entities," and boosterism is repetitious content "created and disseminated to reinforce the perception that a given position represents a popular point of view" (DiResta & Grossman, 2019, p. 5). These tactics rest at the heart of the Kremlin's foreign influence efforts.

The U.S. Department of State's Global Engagement Center (GEC, 2020) organizes Russia's disinformation strategy into five pillars. Those pillars are official government communications, state-funded global messaging, cyber-enabled disinformation, proxy source cultivation, and social media weaponization (GEC, 2020). These activities' explicit connection to the Russian government ranges from clear-cut, such as official government communications, to more covert strategies, such as cyber-enabled forgeries or cloned websites. By employing a combination of overt and covert tactics, the Kremlin's penetration of the information environment is multifold for increased effect.

Analytical Framework Applied to Russian Campaigns

Considering Russia's aims, this section studies Russian online foreign influence in the form of ambient disinformation campaigns, exploitation of social divides, and interference during transitions of power. Ongoing, ambient disinformation plays a critical role in this strategy for amplifying falsehoods' reach. With continuous foreign disinformation, a divided democracy can become a less powerful threat with reduced capacity to withstand further attacks, and this diffusive disinformation strategy can create optimal conditions for more targeted disinformation efforts (Beskow & Carley, 2019). The Kremlin's strategy capitalizes on these advantages by employing long-term, ambient disinformation campaigns against democracies between more targeted information attacks.

Military leaders denote the movement from isolated periods of conflict to persistent information operations from authoritarian powers in the international system.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Current warfare is not always declared but is undeniably already happening (Beskow & Carley, 2019; Gerasimov, 2016). Thus, democracies must be perpetually vigilant about widespread disinformation. The continual nature of Russian disinformation necessitates planning and foresight for successful long-term influence efforts. Researchers suggest the Kremlin organized disinformation activities on social networks far before notable moments, including elections (Kalathil, 2020; Starks, Cerulus, & Scott, 2019). The long-term preparation allows for increasingly effective targeted attacks during moments of particular vulnerabilities. While the exact extent is difficult to quantify, ongoing campaigns continually seek to decay democratic institutions and progress authoritarian vigor.

Influencing Transitions of Political Power

The Kremlin leverages disinformation to influence transitions of political power in the West and neighboring countries, such as during the 2014 Ukrainian Maidan Revolution and the 2016 US presidential election. Russia increased its influence efforts targeting its post-Soviet "near abroad" since the early 2000s, leading to escalation into the Russia–Ukraine war in 2022. This section turns to the 2014 Ukrainian Maidan Revolution to analyze Russian interference during political transitions as part of broader aims still unfolding today.

The 2014 Ukrainian Maidan Revolution

Moscow's efforts to influence nearby post-Soviet countries since the early 2000s include foreign influence campaigns during countries' political transitions. Ukraine is a geographically close democratic target with evident strategic importance to Russia. There is much to learn about the extent of Russian foreign interference across time, including the Kremlin's 2014 to 2016 interference in Ukraine and social media's ongoing role in the Russia–Ukraine conflict.

The 2014 Ukrainian Maidan Revolution was a period of civil unrest and demonstrations in Ukraine, beginning with protests in late 2013 when the Ukrainian government chose not to sign the "Association Agreement and the Deep and Comprehensive Free Trade Agreement with the European Union" (Federal Department of Foreign Affairs, 2020). This protest for greater European integration grew into the removal of Ukraine's pro-Russian President Viktor Yanukovych and unrest over ongoing corruption, human rights violations, and abuses of power (Federal Department of Foreign Affairs, 2020). In response to President Yanukovych's ousting, the Kremlin organized attempts to delegitimize Kyiv's new government and Ukraine's growing inclination to the West through disinformation, proxy war, and militaristic aggression (Sokol, 2019). Through disinformation-heavy influence campaigns, Putin painted adversaries as detesting Jews and the new government as a "fascist junta" spreading antisemitism, racism, and xenophobia (Sokol, 2019, para. 3). This disinformation tactic was significant – and effective – because of World War II's lasting impact throughout the post-Soviet arena.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

The Russian disinformation effort to frame Ukraine's post-revolution leaders as racist and violent occurred at a similar time to when Russia was aiming to conquer the Crimean Peninsula. This invasion of Ukrainian territory and the Crimean annexation began as a Russian state-sponsored media campaign targeting Ukraine (Summers, 2017). Russian disinformation efforts inundated Crimeans with narratives that they were at risk from their fellow people in Kyiv (Yuhas, 2014). This disinformation led many Crimeans to welcome Russian military presence's perceived protection. Disinformation efforts worked to overwhelm the information environment and advance the Kremlin's aims by distracting from their actions and negatively framing others' activities.

A component of this and other Russian campaigns is the ability to morph actual events into a new, carefully crafted narrative removed from reality – but rooted in it and recontextualized. An example is the assertion that Jewish people felt forced to leave Ukraine. While tens of thousands left Ukraine for Israel, as reported by Israeli interior ministry statistics, the departure's motivation was reportedly the danger felt due to Russian aggression, not racism as Russia sought to contrive (Sokol, 2019). Russia maximized the opportunity to frame the exodus as Ukraine's doing and leveraged cyber-enabled attacks to create a perception of chaos and instability within Ukraine (Summers, 2017). Beyond the outside perception of Ukraine, the efforts contributed to Ukrainians' eroding faith in their government and overall unity.

Evidence of the Kremlin propagating anti-Western, pro-Russian content targeting Ukrainians across social media spans years (Chen, 2015; Summers, 2017). The strategically crafted messages from Russia across time and networks showcase the Kremlin's attempts to grow Ukrainian support for Russian interests (Chen, 2015). While it remains a democracy's responsibility to address public opinion within its citizenry, acknowledgment of Russian interference's role in shaping Ukrainians' perceptions is critical.

The 2016 US Presidential Election

The Kremlin's foreign interference attempts are not limited to nearby post-Soviet countries. A highly publicized context of Russian influence campaigns during political transitions is the 2016 US presidential election. Russian interference in the 2016 US presidential election was confirmed by official US government agency investigations, most notably an extensive bipartisan U.S. Senate Intelligence Committee report. Moscow employed a combination of disinformation and hacking intended to push the 2016 US presidential election in favor of Trump (Funke, 2020). Trump became the eventual winner, although assessing how much Russia influenced the outcome from open-source information is challenging. This chapter is less concerned with disinformation's effectiveness as it is with the extent authoritarians deploy campaigns in attempts to influence democracies.

TIME's Shuster (2020) details how Russia initiated a two-pronged attack centered on spreading online disinformation and incorporating cyberattacks to hack the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Democratic Party and election infrastructure. Compared to 2020, the 2016 US presidential election saw more invasive interference with a focus on influence through state-run media and social media disinformation (Shuster, 2020; Wray, 2020). Experts, including the Alliance for Securing Democracy's Bret Schafer, contend that Russia's interference in the 2016 election was stronger than in 2020 because social networks had yet to improve the removal of disinformation-spreading Russian bots and fake accounts (Shuster, 2020). Between 2016 and 2020, American discourse became increasingly divided and fraught with false information and conspiracies originating domestically; thus, Russian efforts in 2016 sowed lasting seeds but arguably did not need to continue amplifying the disinformation already in motion and impacting outcomes (Shuster, 2020).

The U.S. Senate Intelligence Committee shared its final report on Russian influence in the 2016 presidential election in 2020. *The Hill* Staff (2020) published that the report was similar to the findings of the investigation by special counsel Robert Mueller with "overwhelming evidence of Russia's efforts to interfere in the election through disinformation and cyber campaigns but … a lack of sufficient evidence that the Trump campaign conspired with the Kremlin to impact the outcome of the 2016 election." Regarding Moscow's influence in the US 2016 election and Donald Trump's involvement, *Slate*'s Stahl (2020) argues "at the very least, the Trump team was aware of and welcomed this meddling." In-country complicity in foreign disinformation is a complicating factor, as most politicians benefiting from disinformation may be disinclined to intervene or discredit it.

Russian involvement in the 2016 election appears motivated by aims to "tarnish U.S. democracy" and enable Moscow's assertions "Washington has no right telling other nations how to conduct their elections" (Kendall-Taylor & Shullman, 2018, p. 1). Such foreign influence can undermine legitimate democratic processes as people question if events are authentic or resulting from foreign influence. While it is challenging to quantify disinformation campaigns' outcomes, it is undeniable that disinformation's hundreds of millions of social media impressions had lasting effects (*Al Jazeera English*, 2018). Even in the years-later aftermath following Trump's defeat in the 2020 election, 2016's disinformation impacted US sentiments, political views, and rhetoric, including growing distrust and challenges to democratically decided outcomes.

This assessment of Ukraine's 2014 Maidan Revolution and the 2016 US presidential election analyzes Russian disinformation attempting to exploit transitions of political power. These political transitions often include social fractures, and a disillusioned citizenry is vulnerable to adversaries' efforts. The following section focuses on periods of social and cultural divides as democratic vulnerabilities offering powerful opportunities for foreign influence.

Social and Cultural Divides

Social and cultural divides provide periods of vulnerability where adversaries may strike on democracies' existing societal cleavages. These tensions include those

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

between races, religions, political parties, or a country's people and its military (Beskow & Carley, 2019). This section analyzes efforts to capitalize on democracies' social and cultural divides through the Brexit referendum.

Brexit Referendum

An example of alleged Russian interference through disinformation is the United Kingdom European Union referendum, also known as the Brexit referendum in 2016. The UK's Intelligence and Security Committee of Parliament (ISC) investigated Russian interference targeting this social divide (Dearden, 2020). The ISC report uncovered insufficient evidence "Russia meddled to any significant extent . . . nor did Russia influence the final outcome," although it found UK intelligence neglected Russian threats (Castle, 2020, para. 6). The ISC report was complete long before its release, which was delayed until after the general election (Castle, 2020; Ellehuus & Ruy, 2020).

The disinformation-spreading *Strategic Culture Foundation* (SCF) published "editor's choice" articles, such as "The Russian Brexit Plot That Wasn't," to discredit evidence of Russian interference (Robinson, 2020, p. 1). While the extent of Russian disinformation was determined insufficient to sway results, leadership reportedly choosing not to investigate evidence of interference sooner provided a window of opportunity for Russia to bolster its campaigns. Indications of Russian interference in the British government predate the Brexit referendum, including Russian permeation in London, with Castle (2020) referring to the capital as "Londongrad." While Russian interference in the Brexit referendum likely did not alter the vote's outcome, its extent is nonetheless concerning, as is the lack of democratic safeguards from interference in Britain and elsewhere.

CHINESE ONLINE DISINFORMATION CAMPAIGNS TARGETING DEMOCRACIES

Chinese Disinformation's Strategic Aims

Despite authoritarian similarities to Russia, China's strategy maintains unique qualities, making it an attractive second case study. The Chinese Communist Party (CCP) is well-known for its propaganda, censorship, and disinformation (Blumenthal & Zhang, 2020). China's political leaders deny any chance of movement to democracy and favor authoritarian norms. However, China's authoritarian leadership maintains both soft and hard aspects along with self-branding as a "consultative democracy" (Bernstein, 2011; Kim, 2019). While China was previously content to coexist with democracies, its growing power brings a willingness to challenge democracy's broader norms.

The CCP acknowledged that China's military and economic power was insufficient to achieve its aims and turned to increased information warfare through

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

disinformation (Cole, 2019). President Xi lionized "discourse power" to influence narratives and share China's story on the global stage (Rosenberger, 2020, para. 9). Under President Xi, China created a narrative of democracy to grant their political system more "ideological legitimacy" in mainland China, Taiwan, and Hong Kong – and among other communities watching (Kim, 2019, para. 8). There has been a marked increase in the CCP's investment in technologies and its disinformation efforts' intensity in positively branding China.

China increasingly prioritizes the global race for technological advancement. Citing security risks, the United States restricted Chinese companies Huawei and ZTE and encouraged European restriction of their reach (Bartz & Alper, 2022; Mukherjee & Soderpalm, 2020; Shepardson, 2021). Amid this technological power struggle, the CCP expanded its funding for the China Standards 2035 and Made in China 2025 initiatives, aiming to minimize reliance on the United States and promote domestic products (Sinkkonen & Lassila, 2020).

In the State Council Information Office's *White Paper on China's Political Party System*, the CCP shared "socialist democracy" branding, combining consultative and electoral democracy (Kim, 2019, para. 2; USC US-China Institute, 2007). China's vulnerability to criticism spurred leaders to create an image of a democracy differentiated by "Chinese characteristics" instead of blanketly criticizing democracy (Kim, 2019, para. 2). Still lacking specific democratic processes and values, this effort sought to protect China's domestic and international image. Beijing shifted its strategy to project China's system as legitimate and necessary for its prosperity. China's concerns about its global standing contextualize its foreign disinformation strategy.

Kendall-Taylor and Shullman (2018, p. 1) assert that China "used a subtler and more risk-averse strategy, preferring stability that is conducive to building economic ties and influence." This argument contends China's approach focuses on offering resources to weaker democracies to distance them from the West (Kendall-Taylor & Shullman, 2018). These CCP efforts would be less influential without Russian and other countries' concurrent campaigns to erode democratic fixtures.

The CCP's economic, relatively risk-averse, and opportunistic strategies align with this research's examination of Chinese online disinformation. We contend there is a combination of an insufficient public understanding of past foreign interference operations from China coupled with a marked increase in China's disinformation activity in recent years. Kalathil (2020, p. 38) notes the CCP's foreign influence operations were seen as mainly consisting of apparent, innocuous propaganda on official channels for "relatively minimalist and ineffective" outcomes. However, the CCP's approach had likely been oversimplified and underestimated. Kalathil (2020) adds that this analysis ignores China's longtime foreign influence activities to affect the international information environment in their favor.

The CCP seeks to alter broader narratives through private business and journalism, making China's strategy more complex than merely promoting its economic

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

interests. The likely underestimation of China's foreign influence through disinformation partially stems from the deception involved. Evidence of Chinese computational propaganda existed largely within its borders through QQ, WeChat, and Weibo until 2019 (Bradshaw & Howard, 2019). The CCP can maintain power over messaging in China by employing censorship and banning social networks. Despite their ban for Chinese citizens, the CCP's interest in global platforms indicates a wider strategy. Their strategy targets norms, standards, infrastructure, governance, and technology (Kalathil, 2020).

Two central trends of the CCP's disinformation against democracies are a notable rise in disinformation campaigns in recent years and a greater investment in technology for foreign influence. The following sections analyze examples of this shift to include increasingly global platforms and audiences related to our analytical framework's themes of political transitions, societal divides, and ambient disinformation.

Analytical Framework Applied to Chinese Campaigns

Ongoing disinformation proves significant to China's aims to emit a positive reputation. Online campaigns enable China to project favorable information while also burying criticisms. Within China, the CCP can swiftly erase dissenting comments on Chinese platforms while banning other networks. Disinformation allowed China's reach across social networks to grow commensurately with its global stance (Lee Myers & Mozur, 2019). While the CCP can censor and crack down on unwanted information to curate its narrative within China, it can also deploy bots to bury unwanted information and spread pro-CCP messaging across global networks.

In addition to creating supportive press for China and unfavorable press for adversaries, some CCP disinformation aims to deflect attention from China's perceived national failings, including COVID-19's early mishandling, by inundating Chinese and global audiences with heightened campaigns to drown criticisms (Lee Myers & Mozur, 2019; Wallis et al., 2020). Given the CCP's intent to maintain positive narratives and geostrategic relationships globally, ongoing disinformation proves valuable in burying negative commentary and projecting pro-China content.

China–Australia relations provide a compelling example of this strategy. Australia's democracy experienced decades of economic benefits from its relationship with China, including Chinese tourism and student populations (Searight, 2020). However, the revelation of Chinese disinformation to impact Australian politics and discourse stirred the relationship, with some attempts to rebuild trust (Morrison, Barnet, & Martin, 2020; Wallis et al., 2020; Woo, 2023). Evidence revealed CCP-linked disinformation and political donations aspiring to influence major Australian political parties' policies on China (Searight, 2020; Wallis et al., 2020). Because China's ongoing disinformation and soft power in Australia are

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

pervasive, this dynamic presents economic and security challenges for their relationship's future.

While these ongoing disinformation efforts targeting democracies serve as a backdrop to the international system, there are marked periods when China opportunistically exploits democratic vulnerabilities through societal divisions. This chapter next analyzes Taiwan as a case of Chinese influence during political transition before assessing the Hong Kong protests as Chinese influence during social and cultural divides.

Influencing Transitions of Political Power

China's relationship with Taiwan and Hong Kong is contested and complex; therefore, this research acknowledges China's disinformation against Taiwan and Hong Kong's pursuit of democracy as having both domestic and international aspects (Hernández & Lee Myers, 2020; Horton, 2019). With different political systems, Taiwan and Hong Kong showcase examples of China's interference in democratic institutions through disinformation.

Taiwan

Taiwan presents a timely example of China targeting its influence operations at democratization and political transitions. Themes of China's online disinformation include undermining Taiwan's ruling Democratic Progressive Party (DPP) and President Tsai Ing-wen (Steger, 2020). The CCP recognized Taiwan's democratization complicates its aims to acquire control of Taiwan (Cole, 2019). China is willing to pursue great lengths to interrupt Taiwan's democratization, including military force and information warfare (Hernández & Lee Myers, 2020).

Inaccurate information across Facebook, YouTube, and Twitter (now X) targeted Taiwan's democratic institutions, including presidential elections and DPP leadership. Wallis et al. (2020) uncovered increased Twitter accounts created by China's Ministry of Foreign Affairs diplomats, spokespeople, state media, and embassies through 2018 and 2019. Disinformation from China included homophobic rumors regarding President Tsai Ing-wen's sexuality. These disinformation attacks capitalized on the resentment some citizens felt toward her policies supporting LGBTQIA + rights (Steger, 2020). Fact-checking organizations debunked unfounded claims; however, closed messaging groups' popularity throughout Taiwan proved troublesome as users could privately forward untrue information (Steger, 2020).

Taiwan's response showcases an instructive model for fighting foreign influence from disinformation. Taiwan fined CtiTV, a primary cable network, in response to inadequate fact-checking and created its Department of Cyber Security and ministry-specific disinformation detection task forces (Halpert, 2020). Before Taiwan's 2020 presidential election, the country passed the Anti-Infiltration Act to impose potential fines and prison sentences for actors peddling disinformation, obstructing elections, or interfering with international politics (Halpert, 2020).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

China's Taiwan Affairs Office spokesperson asserted the act generates "panic that everyone is treated as an enemy" and China has never engaged in "elections in the Taiwan region" (*Reuters*, 2019, para. 6). The wording of the "Taiwan region" rejects its autonomy, and the framing of this policy as hurting "everyone" offers context to inform our analysis. The "infiltration sources" Taiwan's legislation aims to protect against are understood to mean Chinese interference (*Reuters*, 2019, para. 4). Taiwanese media focuses on Chinese intelligence as a key player in discrediting Taiwan President Tsai Ing-wen and her advocacy for Taiwan's independence (Aspinwall, 2020). Taiwan's efforts to institute anti-disinformation laws in reaction to China follow examples from Finland and Estonia as recipients of Russia's foreign influence through disinformation (Aspinwall, 2020).

Taiwan's societal divides aid Chinese disinformation's effectiveness, such as disinformation against LGBTQIA+-supporting Taiwanese President Tsai Ing-wen leveraging certain citizens' homophobic sentiments. Taiwan's 2020 election depicts a period of vulnerability through the potential transition of power, which overlaps with societal divides the CCP exploited to undermine Taiwan's president. These divisions present opportunities for further analysis of Chinese influence against democratic institutions.

Social and Cultural Divides

HONG KONG PROTESTS. In recent decades, grassroots protests became increasingly menacing for authoritarian regimes. Hong Kong presents a noteworthy case of Chinese interference in democracy. There appears to be a three-pronged approach to China's online disinformation targeting Hong Kong: (1) accusations that the protesters are dangerous and violent, (2) allegations of United States and other interference being involved, and (3) demands to support the police in Hong Kong and undermine protests (Wallis et al., 2020).

The CCP's strategy shifted from efforts to contain democracy in Hong Kong to more direct control, influencing its use of disinformation to be more interventionist. Chinese responses to the Hong Kong protests were to increasingly suppress opposition, especially through technological methods, including disinformation amplification on social networks (Sinkkonen & Lassila, 2020). In 2019, China's government incorporated worldwide social media platforms to paint democracy advocates in Hong Kong as violent radicals lacking popular opinion (Bradshaw & Howard, 2019; Lee Myers & Mozur, 2019). Digital repression has not entirely eclipsed physical means of influence but offers new opportunities for attacks against adversaries (Sinkkonen & Lassila, 2020). Disinformation is a dangerous method for regimes to distort or otherwise control narratives about the extent of physical measures, popular opinion, and other forms of interference. Twitter and Facebook removed various accounts tied to the CCP's efforts to undermine the protests in Hong Kong, and Twitter announced policies to prohibit "state-controlled news media" advertisements

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

(Halpert, 2020; Twitter Inc., 2019). However, limited staff, scale, and other factors complicate timely response.

China shared content through social and state media to increase nationalist and anti-Western views. This strategy includes manipulating photos and videos to subvert protesters or label the protests as a dangerous gateway to terrorism (Lee Myers & Mozur, 2019). In mid-2019, Twitter, Facebook, and YouTube uncovered and suspended accounts tied to Beijing propagating Hong Kong protest disinformation (Alba & Satariano, 2019). These efforts intensified opposing views. As seen from Hong Kong, the demonstration movement was popular. However, the Chinese perspective led people to believe a violent, small group of radicals yearned to tear China apart.

As China advances its disinformation strategy, it likewise increases its expertise and ability to leverage social media's reach to networks worldwide. The CCP employs teams of citizens to "actively shape public opinions and police speech through online channels" (Bradshaw & Howard, 2019, p. 17). Networks of people and bots amplify disinformation to manipulate opinion (Alba & Satariano, 2019). China invests in professionalizing its disinformation tactics, including formal organizations with hiring plans and bonuses for performance (Alba & Satariano, 2019).

These data support the conclusion that China uses social media networks to exert influence and power worldwide, particularly regarding claims of land in Taiwan and Hong Kong as its sovereign territory. The extent of Chinese disinformation campaigns aimed at these regional territories reflects the aims and energy of the CCP to such ends until recently. These geographically close and territory-based ends are critical, but they are not the only form of influence operations as China's aims evolve with its growing geostrategic power.

ANALYSIS AND INSIGHTS

Our analytical framework is applicable across authoritarian contexts and finds certain similarities in its analysis of Russian and Chinese disinformation. Moscow and Beijing are both prominent disinformation-propagating actors in the international system, and they target robust Western democracies and neighboring states of strategic importance. However, it would be a mistake to assume the substance, aims, and contexts of these different authoritarian states' disinformation campaigns are neatly comparable. Each authoritarian state – and democratic target – has specific complexities.

While this research's analytical framework offers valuable insight broadly, there are core differences in how, to what aims, and to what extent these authoritarian states deploy their disinformation campaigns. Russia and China may share interests in diminished Western powers and antidemocracy efforts, but different ideologies and objectives drive the states' activities (Jeangène Vilmer & Charon, 2020). Each authoritarian state's disinformation campaigns against democracies requires analysis within the dyadic relationship between the authoritarian state and the target of its disinformation.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Distinguishing Aims and Leadership Profiles

While Russia and China's disinformation campaigns share similar strategic aims, they may or may not use similar strategies. Broadly speaking, Russia builds on its longstanding history of propaganda for a more direct, manipulation-driven approach, while China invested heavily in technological innovation more recently for a gradual, permeating, censorship-driven approach. The CCP prioritizes its efforts to show China's global image as respectable, uncorrupt, and morally sound and subdues content indicating otherwise (Jeangène Vilmer & Charon, 2020). Russia is less concerned with its image and appears as a "well-armed rogue state" aiming to disrupt the present international order (Dobbins, Shatz, & Wyne, 2019, para. 1). While China seeks increasing power, it is less concerned with Russia's goals to disrupt the system because it holds greater power and faces steeper reputational risks. Part of Russia's impetus for disinformation is its weakening global stance and lack of benefits from the present international order (Jeangène Vilmer & Charon, 2020). The Kremlin is thus willing to embrace risks in its disinformation strategy to disrupt the system for greater power and influence.

In contrast to Russia, China more strategically prioritized economic relationships, including investment, trade, and development assistance, to grow its influence in the international system (Dobbins, Shatz, & Wyne, 2019). China's export of products and services aids the country financially and helps develop other countries' relationships with – and dependency on – China. Chinese exports' breadth showcases Beijing's infrastructure investments to lead technologically and globally (Sinkkonen & Lassila, 2020). China's Belt and Road Initiative incorporates a Digital Silk Road component to further Chinese global advancement (Greene & Triolo, 2020). These relationships make China more risk-averse, reputation-oriented, and gradual in its disinformation than Russia.

China holds a more dominant role in the current international order and must be more careful and less overtly aggressive in its strategy. Despite their deflection and denial, Russia and China do little to hide their interference efforts because there is little need. With low costs, lack of gatekeepers, and accessible social networks, disinformation is an alluring way to further aims with relative anonymity (Garcia, 2020). While research indicates the most likely source of disinformation against a specific democracy, exact proof of culpability is challenging. The disinformation-deploying state can evade consequences by denying responsibility while inflicting ramifications on the targeted state.

If President Xi's foreign policy becomes more aggressive, these differences in Russian and Chinese aims may shrink. For the first time in July 2021, China announced sanctions against Western institutions criticizing them (Rudd, 2022). Another example is China's growing interest in near abroad territories and lack of concern for positive relations with certain democracies, particularly Taiwan. Rudd (2022, para. 3) contends "ideology drives policy more often than the other way

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

around" under Xi's leadership, and he seeks to strengthen the Communist Party by stirring nationalism and asserting foreign policy to solidify China's power. In contrast, President Putin projects a "clever, manipulating strongman" image to protect his power as a ruler (Kovalev, 2023, para. 4). A strongman losing the appearance of might could lead to drastic action or demise. The Russia–Ukraine war, especially the Wagner Group rebellion, prompted doubts about Putin's crafted image (Kovalev, 2023; Sly, 2023). While Putin moves to preserve his leadership status, Xi appears driven by a "Marxist-inspired belief" that Chinese strength means a "more just international order" (Rudd, 2022, para. 3). These approaches centering the person versus the party lead to different strategies for authoritarianism.

While it is unlikely that China will forgo its priority of positive international relations, President Xi is likely watching the Russia–Ukraine war closely as it assesses possible territorial moves. While analysis of disinformation campaigns needs to happen within the individual dyads of the instigating state and the targeted state, it is useful to analyze the extent of partnerships between or among authoritarian states in pursuing their interests to undermine democracy. This is especially true when interests align, such as Russia in Ukraine and China in Taiwan for territorial conquests.

Power Relations and Strategic Cooperation

This inquiry requires analysis of strategic cooperation between authoritarian states to target democracies. China and Russia share a border and adversarial US relations, with Xi and Putin projecting an "intimate" friendship (Lau, 2023, para. 1). Russia and China's agendas share aims to influence the hallmarks of democracy, including free speech and public debate. Both measure their power relative to Western democracies, meaning that weakened democracy could increase their strength (Kendall-Taylor & Shullman, 2018). Both states leverage disinformation to legitimize authoritarian systems and delegitimize democratic systems. While some cooperation between Russia and China exists, this dynamic is more nuanced than simply an authoritarian alliance. Despite sharing similar adversaries, authoritarian regimes are also competing with each other.

Disinformation-propagating authoritarian regimes learned from each other's anti democracy campaigns, especially from Russia under Putin, to grow more robust disinformation strategies. With the Russian government's disinformation appearing as the most visible, it is understandable yet simplistic to apply the same motivations to China. China is unlikely to cooperate extensively with Russia and its aggressive approach for fear of losing its dominant position in the international trading system. Unless necessary, the CCP will likely tread carefully to avoid harming its economic and strategic relationships.

While priorities differ, authoritarian states' collective efforts create a "more corrosive effect on democracy than either would have single-handedly" (Kendall-Taylor

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

& Shullman, 2018, p. 1). Russia and China's aims are specific to their regimes, yet they operate within the same antidemocratic ecosystem. Without Russian campaigns to erode global commitment to democracy and democratic institutions, China's foreign interference efforts would likely be less powerful (Kendall-Taylor & Shullman, 2018).

Some experts designated 2020 and 2021 as "years for Russian–Chinese science cooperation with the focus on communications, AI and the Internet of Things" building off of past partnerships like 2019's "Sino-Russian Joint Innovation Investment Fund" (Sinkkonen & Lassila, 2020, p. 6). As much of this cooperation would presumably occur in private due to disinformation's deceptive nature, we lack concrete evidence of the extent the governments are strategically cooperating.

As there are moving pieces to disinformation campaigns and the states' individual aims vary, coordination may not be necessary. Russia, China, and other authoritarian states can and do act independently and amplify each other when it aligns with individual interests (Jeangène Vilmer & Charon, 2020). Given Beijing's central aim to promote pro-CCP messaging, it is unlikely Moscow would spread pro-CCP propaganda without benefiting the Kremlin or eroding adversaries' powers. Although antidemocracy disinformation serves both states' interests, applying a blanket model to authoritarian regimes' influence operations would be a disservice to countering interference.

Resilience and Democracy

Foreign interference efforts from authoritarian states have implications for democratic health and vulnerabilities, and democracies must take preemptive steps to protect themselves. There are multiple technical and governance strategies that democracies can consider to increase resiliency against targeted disinformation campaigns (RAND Corporation, 2023). Two useful methods are improved digital and media literacy among citizens and partnership-building across affected sectors and countries. Creating and promoting information literacy support for citizens can reduce vulnerabilities to disinformation. Especially in recent years, practitioners created resources for citizens to safely navigate the online information environment, including IREX's Learn 2 Discern curriculum, Stanford's Putting Civic Online Reasoning Program initiative, Google's Interland, and the News Literacy Project's Checkology curriculum (Brooks, 2020; News Literacy Project, 2023; RAND Corporation, 2023; Stanford History Education Group, 2023). Civil society education alone is insufficient against targeted online disinformation, but greater information literacy is vital for democracies to stay resilient against foreign interference (Brooks, 2020).

Another means to reduce democratic vulnerabilities to online disinformation is through partnerships. Much like disinformation-propagating outlets partnered to spread their nefarious content, collaboration among reputable outlets can reduce

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

democratic vulnerabilities. For disinformation happening in the context of Hong Kong or Ukraine, partnerships between citizen journalists and mainstream media can strengthen the quality of information (Brooks, 2020; Huang, 2020). In places where high-risk geopolitical events or other conditions make international reporting challenging, networks of trusted citizen journalists are critical to mitigating erroneous information and reporting timely authentic news (Visram, 2020).

By combining education and partnerships, Taiwan's response showcases a whole-of-society approach to combating Chinese disinformation (Huang, 2020). The creation of laws, notably the Anti-Infiltration Act, imposed potential prison sentences and heavy fines for people spreading disinformation (Aspinwall, 2020; Halpert, 2020). Taiwan's institutional approach formed ministry-specific disinformation detection task forces and supported programs led by Taipei's digital minister. Other countries implemented other forms of regulations and protections, and democracies should continue to assess what models work best for their online and in-country contexts.

For democracies to stay healthy and competitive against targeted disinformation, they must create policies and safeguards to protect the free flow of reliable information online. Sokol (2019, p. 1) describes how successful disinformation campaigns are "based on a core of truth . . . distorted and exaggerated beyond recognition." The challenge of disinformation requires democracies to protect their institutions in mundane times and times of greatest vulnerability. So long as they support transparency, public debate, and free speech, democracies will likely remain targets of disinformation. By addressing the root of divisions within democracies, they have greater resiliency to foreign influence efforts.

CONCLUSION

Technology has become a permanent fixture in society and will continue to pose opportunities – and challenges – to the international system. As new technologies evolve, so must democracies to stay resilient against foreign adversaries' attempts to weaken democratic institutions through disinformation.

This research analyzed the extent to which and how foreign online disinformation campaigns target democracies, specifically disinformation from the Russian and Chinese governments toward specific democracies. We found Russia is a manipulation-driven, rogue state with a history of disinformation aiming to disrupt the international order as it senses its slipping power. China likewise seeks increasing power, yet is less concerned with disrupting the international system because it holds a more powerful global position and deploys a more gradual, censorship-driven approach.

Assessing authoritarian states' online disinformation campaigns through the same analytical framework proves useful; yet assuming all authoritarian states operate similarly is a mistake. Each authoritarian state's disinformation campaigns

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

necessitate assessment within dyadic relationships between disinformation-propagating states and their targets. Examples of democracies targeted by Russia and China fit into our analytical framework of long-term, ambient disinformation, transitions of political power, and social and cultural movements. They also exposed patterns in targets primarily categorized as either Western powers or neighboring states of strategic importance.

The main distinctions between Russia and China and their various targets reflect different aims, objectives, risks, and contexts for using targeted disinformation depending on the target state. Another line of argumentation is that disinformation-propagating authoritarian regimes learned from each other's campaigns and partnered to some extent in antidemocracy efforts. While Russia and China may share interests in authoritarianism and diminished Western powers, different ideologies, objectives, and relationships drive them. Cooperation among authoritarian states appears to be out of convenience more than partnership, as they are simultaneously competing with each other.

Russia and China present two of the authoritarian powers most threatening to democracies with their strong capacities to deploy antidemocratic disinformation. Russia appears as a more immediate and brazen threat; however, China presents a long-term threat to democracies as it strategically grows its geopolitical power. China is more concerned with promoting its positive image and creating reasonable working relations with Western democracies than Russia's abrasive approach. The recent progress in China's disinformation ecosystem merits continued analysis in the coming years, coupled with lessons learned from Russia's extended disinformation ecosystem, particularly in the Russia–Ukraine war. Application of this research's analytical framework to other authoritarian regimes, including Iran and North Korea, can assess additional influence efforts.

A healthy democracy relies on trust and access to quality information. Social networks drastically changed the information environment, offering opportunities for increased online information and disinformation. We found varying authoritarian strategies to undermine faith in democratic processes through disinformation. The extent to which these efforts swayed outcomes is tangential to how these campaigns worsened societal divides and eroded trust among citizens. Even the most resilient democracies must protect themselves and their information environments against the ongoing threat of foreign interference.

REFERENCES

Al Jazeera English. (2018, February 1). *Disinformation and democracy (part I), People and power*. YouTube. https://youtube.com/watch?v = eZEz6Pc3Z24

Alba, D., & Satariano, A. (2019, September 26). At least 70 countries have had disinformation campaigns, study finds. *The New York Times*. https://nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Aspinwall, N. (2020, January 10). Taiwan's war on fake news is hitting the wrong targets. *Foreign Policy*. https://foreignpolicy.com/2020/01/10/taiwan-election-tsai-disinformation-china-war-fake-news-hitting-wrong-targets/

Bartz, D., & Alper, A. (2022, November 30). *U.S. bans new Huawei, ZTE equipment sales, citing national security risk*. Reuters. https://reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/

Bernstein, T. (2011, April 11). *Video: Varieties of authoritarianism – Comparing China and Russia*. USC US-China Institute. https://china.usc.edu/video-varieties-authoritarianism-comparing-china-and-russia

Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity an emerging national security requirement. *Military Review*. March–April 2019, pp. 117–127. https://armyupress.army.mil/Portals/7/military-review/Archives/English/MA-2019/Beskow-Carley-Social-Cyber.pdf

Blumenthal, D., & Zhang, L. (2020, July 10). *China's censorship, propaganda & disinformation*. Jewish Policy Center. AEI. https://aei.org/articles/chinas-censorship-propaganda-disinformation

Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*. University of Oxford. Computational Propaganda Research Project. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf

Brooks, R. (2020). *Research Plan & Weekly Updates. Research Fellowship: Digital Threats to Election Integrity*. The Carter Center Democracy Program. Unpublished research.

Castle, S. (2020, July 21). Five takeaways from the report on Russia's interference in Britain. *The New York Times*. https://nytimes.com/2020/07/21/world/europe/uk-russia-report-takeaways.html

Chen, A. (2015, June 7). The agency. *The New York Times*. https://nytimes.com/2015/06/07/magazine/the-agency.html

Cole, J. M. (2019). *Chinese disinformation in Taiwan*. Taiwan Sentinel. https://sentinel.tw/chinese-disinformation-in-taiwan

Dearden, L. (2020, July 21). *Russia report: Moscow's disinformation campaign fuelling 'political extremism' and division in UK*. The Independent. https://independent.co.uk/news/uk/home-news/russia-report-uk-national-security-brexit-terror-islam-a9630126.html

DiResta, R., & Grossman, S. (2019). *Potemkin pages & personas: Assessing GRU online operations, 2014–2019*. Stanford: Internet Observatory Cyber Policy Center. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf

Dobbins, J., Shatz, J., & Wyne, A. (2019). *Russia is a rogue, not a peer; China is a peer, not a rogue: Different challenges, different responses*. RAND Corporation. https://rand.org/pubs/perspectives/PE310.html

Ellehuus, R., & Ruy, D. (2020, July 21). *Did Russia influence Brexit?* Center for Strategic and International Studies (CSIS). https://csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit

Federal Department of Foreign Affairs. (2020). *Swiss Cooperation Programme Ukraine 2020–23*. Swiss Confederation. https://eda.admin.ch/dam/deza/en/documents/laender/cooperation-programme-ukraine_EN.pdf

Funke, D. (2020, September 25). *What we know about 2020 election interference: It's not just Russia*. Politifact: The Poynter Institute. https://politifact.com/article/2020/sep/25/what-we-know-about-2020-election-interference-its

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Garcia, C. (2020, April 17). *Untangling the disinformation problem: Russia, China and the West*. The Wilson Center. https://wilsoncenter.org/blog-post/untangling-disinformation-problem-russia-china-and-west

GEC (2020). *GEC special report: August 2020 pillars of Russia's disinformation and propaganda ecosystem*. U.S. Department of State. https://state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

Gerasimov, V. (2016). The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. *Military Review*. January –February 2016 , pp. 23 –29. https://state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

Greene, R., & Triolo, P. (2020, May 8). *Will China control the global internet via its Digital Silk Road?* Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

Halpert, D. (2020, April 8). *Disinformation prevention and defending democracy in Taiwan*. Brown Political Review. https://brownpoliticalreview.org/2020/04/disinformation-prevention-and-defending-democracy-in-taiwan/

Hernández, J. C., & Lee Myers, S. (2020, July 1). As China strengthens grip on Hong Kong, Taiwan sees a threat. *The New York Times*. https://nytimes.com/2020/07/01/world/asia/taiwan-china-hong-kong.html

Horton, C. (2019, July 5). Hong Kong and Taiwan are bonding over China. *The Atlantic*. https://theatlantic.com/international/archive/2019/07/china-bonds-between-hong-kong-and-taiwan-are-growing/593347/

Huang, A. (2020, July). *Combatting and defeating Chinese propaganda and disinformation: A case study of Taiwan's 2020 elections*. Belfer Center for Science and International Affairs at the Harvard Kennedy School. https://belfercenter.org/sites/default/files/files/publication/Combatting%20Chinese%20Propaganda%20and%20Disinformation%20-%20Huang.pdf

Jeangène Vilmer, J.-B., & Charon, P. (2020, January 21). *Russia as a hurricane, China as climate change: Different ways of information warfare*. War on the Rocks. https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/

Kalathil, S. (2020). The evolution of authoritarian digital influence: Grappling with the new normal. *PRISM*, 9(1), 33 –50. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_33-50_Kalathil-2.pdf?ver = DJRX5DRHKfqeXbyt6et98w%3D%3D

Kendall-Taylor, A. & Shullman, D. O. (2018, October 2). *How Russia and China undermine democracy*. Foreign Affairs. https://foreignaffairs.com/articles/china/2018-10-02/how-russia-and-china-undermine-democracy

Kim, J. (2019, December 6). Exploring China's new narrative on democracy. *The Diplomat*. https://thediplomat.com/2019/12/exploring-chinas-new-narrative-on-democracy/

Kovalev, A. (2023, June 27). *Putin's strongman image suddenly unravels for Russians*. Foreign Policy. https://foreignpolicy.com/2023/06/27/putin-prigozhin-wagner-mutiny-weakness-russians-opposition-war-ukraine/

Lau, S. (2023, March 20). Why Xi Jinping is still Vladimir Putin's best friend. *Politico*. https://politico.eu/article/xi-jinping-china-vladimir-putin-russia-best-friend-ally-war-in-ukraine/

Lee Myers, S., & Mozur, P. (2019, August 13). China is waging a disinformation war against Hong Kong protesters. *The New York Times*. https://nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Morrison, S., Barnet, B., & Martin, J. (2020, June 23). *China's disinformation threat is real. We need better defences against state-based cyber campaigns*. The Conversation. https://theconversation.com/chinas-disinformation-threat-is-real-we-need-better-defences-against-state-based-cyber-campaigns-141044

Mukherjee, S., & Soderpalm, H. (2020, October 20). *Sweden bans Huawei, ZTE from upcoming 5G networks*. Reuters. https://reuters.com/#:~:text=STOCKHOLM%20(Reuters)%20%2D%20Sweden%20has,Chinese%20suppliers%20on%20security%20grounds

News Literacy Project. (2023). *Checkology*. News Literacy Project. https://newslit.org/educators/checkology/

Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality*. PublicAffairs. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3108041/this-is-not-propaganda-adventures-in-the-war-against-reality/

RAND Corporation. (2023). *Tools that fight disinformation online*. RAND Corporation. https://rand.org/research/projects/truth-decay/fighting-disinformation/search.html

Reuters. (2019, December 10). *China says Taiwan anti-infiltration bill causes 'alarm' for investors*. Reuters. https://reuters.com/article/us-china-taiwan-idUSKBN1YF09Y

Robinson, P. (2020, November 27). *The Russian Brexit plot that wasn't*. Strategic Culture Foundation. https://strategic-culture.org/news/2020/11/27/the-russian-brexit-plot-that-wasnt/

Rosenberger, L. (2020). Disinformation disorientation. *The Journal of Democracy*, *31*(1), 203 – 207.

Rudd, K. (2022, October 10). *The World According to Xi Jinping*. Foreign Affairs. https://foreignaffairs.com/china/world-according-xi-jinping-china-ideologue-kevin-rudd

Sanger, D. and Kanno-Youngs, Z. (2020, September 22). The Russian trolls have a simpler job today. Quote Trump. *The New York Times*. https://nytimes.com/2020/09/22/us/politics/russia-disinformation-election-trump.html

Searight, A. (2020, May 8). *Countering China's influence operations: Lessons from Australia*. CSIS. https://csis.org/analysis/countering-chinas-influence-operations-lessons-australia

Shepardson, D. (2021, November 11). *Biden signs legislation to tighten U.S. restrictions on Huawei, ZTE*. Reuters. https://reuters.com/technology/biden-signs-legislation-tighten-us-restrictions-huawei-zte-2021-11-11/

Shuster, S. (2020, October 7). *What U.S.-Russia talks on election meddling say about the Kremlin's shifting strategy*. TIME. https://time.com/5897310/russia-us-election-interference/

Sinkkonen, E., & Lassila, J. (2020). *Digital authoritarianism in China and Russia: Common goals and diverging standpoints in the era of great-power rivalry*. Finnish Institute of International Affairs. FIIA Briefing Paper 294. https://fiia.fi/en/publication/digital-authoritarianism-in-china-and-russia

Sly, L. (2023, June 28). Putin's standing as global strongman in jeopardy after revolt. *The Washington Post*. https://washingtonpost.com/world/2023/06/28/putin-strongman-image-damaged/

Sokol, S. (2019, August 2). *Russian disinformation distorted reality in Ukraine. Americans should take note*. Foreign Policy. https://foreignpolicy.com/2019/08/02/russian-disinformation-distorted-reality-in-ukraine-americans-should-take-note-putin-mueller-elections-antisemitism/

Stahl, J. (2020, August 18). The top five "revelations" of the Senate Intelligence Committee's Russia Report. *Slate*. https://slate.com/news-and-politics/2020/08/senate-intelligence-russia-report-mueller-comparison.html

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Stanford History Education Group. (2023). *Civil online reasoning: Sorting fact from fiction on the internet*. Stanford History Education Group at Stanford University Graduate School of Education. https://online.stanford.edu/courses/gse-xsheg0006-civic-online-reasoning-sorting-fact-fiction-internet

Starks, T., Cerulus, L., & Scott, M. (2019, June 5). Russia's manipulation of Twitter was far vaster than believed. *Politico*. https://politico.com/story/2019/06/05/study-russia-cybersecurity-twitter-1353543

Steger, I. (2020, January 6). *Taiwan's president is battling a deluge of election-linked homophobic fake news*. Quartz. https://qz.com/1780015/taiwan-election-tsai-ing-wen-faces-homophobic-fake-news/

Stolberg, S. G., & Weiland, N. (2020, September 30). Study finds 'single largest driver' of coronavirus misinformation: Trump. *The New York Times*. https://nytimes.com/2020/09/30/us/politics/trump-coronavirus-misinformation.html

Sukhankin, S. (2019). The Western alliance in the face of the Russian (dis)information machine: Where does Canada stand? *University of Calgary: The School of Public Policy Publications*, *12*(26), 1–31. https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 3454249

Summers, J. (2017, October 25). *Countering disinformation: Russia's infowar in Ukraine*. The Henry M. Jackson School of International Studies at the University of Washington. https://jsis.washington.edu/news/russia-disinformation-ukraine/

The Hill Staff. (2020, August 18). Read: Final Senate Intelligence Committee report on Russian election interference. *The Hill*. https://thehill.com/policy/national-security/512493-read-final-senate-intelligence-committee-report-on-russian-election

Theohary, C. A. (2018, March 5). *Information warfare: Issues for Congress*. Congressional Research Service. https://fas.org/sgp/crs/natsec/R45142.pdf

Twitter Inc. (2019, August 19). *Updating our advertising policies on state media*. Twitter. https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html

U.S. Department of Homeland Security (2020). *Homeland threat assessment*. U.S. Department of Homeland Security. https://dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

USC US-China Institute. (2007, November 15). *White paper on China's political party system*. USC US-China Institute at USC Annenberg. https://china.usc.edu/white-paper-chinas-political-party-system-2007

Visram, T. (2020, June 29). *Citizen journalists are documenting COVID in the world's conflict zones to stop disinformation*. Fast Company. https://fastcompany.com/90521383/citizen-journalists-are-documenting-covid-in-the-worlds-conflict-zones-to-stop-disinformation

Wallis, J., Uren, T., Thomas, E., Zhang, A., Hoffman, S., Li, L., Pascoe, A., & Cave, D. (2020, June). *Retweeting through the great firewall: A persistent and undeterred threat actor*. Australian Strategic Policy Institute. International Cyber Policy Centre. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall_0.pdf?zjVSJfAOYGRkguAbufYr8KRSQ610SfRX

White House (2015, February). *National security strategy*. Obama White House Archives. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy.pdf

Woo, R. (2023, November 6). *China, Australia agree to turn the page as tensions ease*. Reuters. https://reuters.com/world/asia-pacific/australias-albanese-retraces-historic-beijing-walk-visit-mend-ties-2023-11-06/

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004

Wray, C. (2020, September 17). *Worldwide threats to the homeland*. Federal Bureau of Investigation. Statement before the House Homeland Security Committee. Washington, D C. https://fbi.gov/news/testimony/worldwide-threats-to-the-homeland-091720

Yuhas, A. (2014, March 17). Russian propaganda over Crimea and the Ukraine: How does it work? *The Guardian*. https://theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 02:22:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.004