The Heritage Foundation

BACKGROUNDER
No. 3815 | FEBRUARY 21, 2024
ASIAN STUDIES CENTER

South Korea Must Counter Chinese Influence Operations—and the U.S. Should Provide Support

Bruce Klingner

KEY TAKEAWAYS

Chinese covert influence and disinformation operations are a threat to South Korean liberal democracy and U.S. strategic interests in the Indo–Pacific.

Beijing seeks to erode public confidence in democratic institutions, divide America's allies, and undermine resistance to China's aggressive expansionist policies.

Targeting Chinese disinformation campaigns in South Korea can be the foundation of a larger effort to counteract this problem globally.

China is engaging in a global campaign to manipulate foreign public opinion, government policies, and election results through overt and covert means. The multi-faceted strategy uses licit and illicit means of persuasion and coercion including public diplomacy, propaganda, soft power, economic influence, weaponization of trade, disinformation, and influence operations.

Beijing sways foreign think tanks, researchers, and scholars to a more pro-China viewpoint by providing—or threatening to withhold—financial support, visas for travel to China, and access to Chinese officials and academics.

China threatens or imposes severe economic consequences to impel foreign decision-making into compliance with Beijing's objectives. South Koreans frequently cite China's economic retaliation to

Seoul's 2017 decision to host the U.S. Terminal High Altitude Area Defense (THAAD) missile defense system as the rationale for South Korea's continuing timidity in criticizing Chinese human rights violations and coercive actions in the East and South China Seas.

China uses tough "wolf warrior" messages[1] while portraying itself as a victim of Western containment strategy in its official media and diplomatic messages to alter foreign opinions. Chinese government agencies and state media overtly collaborate with foreign media outlets to distribute Chinese-produced content.

However, Beijing realizes the limits of official messaging and employs covert influence operations to augment the impact of government themes while obscuring their sourcing. The *sub rosa* programs are distinguished by being "covert, coercive or corrupt."[2]

Beijing manipulates foreign public policy debates and influences elections by spreading disinformation while discrediting legitimate news, intensifying political differences within target countries, and inflating public support for a politician or party. Chinese overseas influence operations can have specific policy objectives or, more broadly, seek to improve foreign opinions of China, stoke domestic political and social tensions, undermine support for the national government, sow distrust of the electoral system, or weaken support for alliances and partnerships with the United States.

While the United States and Taiwan are primary targets of Chinese influence operations, Beijing also attacks other American allies and partners to discredit the U.S., increase China's influence in the global south, undermine Washington's efforts to promote regional stability, and rebuff China's coercive strategies. South Korea, for example, is a key American ally against the North Korean threat and increasingly opposed to China's coercive policies in the Indo–Pacific.

China's long-standing objective of dividing Seoul from Washington took on greater urgency with the election of conservative President Yoon Suk Yeol in May 2022. Yoon reversed the policies of his left-of-center predecessor by strengthening the alliance with the United States, implementing a principled policy toward North Korea, and improving relations with Japan to enable stronger trilateral security cooperation. Yoon firmly aligned South Korea with the United States and other like-minded democracies, notably Japan, in opposing China's efforts to intimidate Asian nations.

Beijing would see great benefit to covertly influencing South Korean public opinion in the run-up to the April 2024 National Assembly and 2027 presidential elections in favor of progressive candidates whose policies

more closely align with Chinese objectives. By exacerbating domestic resistance to President Yoon's conservative policies, Beijing could hinder his foreign and security agendas.

The United States should closely coordinate with South Korea to combat China's covert efforts to sow discord between Washington and Seoul. For its part, the Korean government should implement a multifaceted strategy to reduce Beijing's ability to alter South Korean public opinion, government policies, and election results. Seoul's efforts, however, must be carefully crafted to avoid impinging on civil rights or censoring legitimate public criticism of the government. Both the government's and tech companies' efforts must be directed against malignant Chinese influence operations rather than stifling populace dissent of administration policies or personnel.

China's Covert Influence Strategy

China has greatly expanded the scope and intensity of its influence operations. In 2021, President Xi Jinping directed Chinese state media to strengthen their propaganda and tailor "precise communication methods" to influence foreign audiences globally.[3] The government now spends billions of dollars annually on foreign information manipulation.[4]

The U.S. Director of National Intelligence assessed that China is becoming "more aggressive" with its covert influence campaigns and using a "sophisticated array of covert, overt, licit, and illicit means [to]sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence, particularly in East Asia and the western Pacific, which Beijing views as its sphere of influence."[5]

Beijing uses an extensive number of government organizations and non-state actors to disseminate its propaganda and disinformation. Most prominent of these is the Chinese Communist Party's (CCP's) United Front Work Department, which the Chinese government described as "a big magic weapon which can rid us of 10,000 problems in order to seize victory."[6]

China provides free video footage and television scripts to 1,700 foreign news organizations as well as English-language articles in order to place government-created products in influential foreign media. But Beijing launders their origin by attributing them to sources without any discernible link to China. Chinese officials then use state media or unofficial accounts to amplify and promote the manufactured opinions.[7] Beijing strives to add credibility to its propaganda themes by making them appear to have come from foreign sources.

The regime also uses social media platforms, such as Internet chat forums and social networking sites, to manipulate foreign opinion. Beijing creates numerous false accounts and uses media influencers—many of whom are Chinese government media employees—to generate support for Chinese policies or counter critics. The regime maintains networks of fake accounts and automated software programs ("bots") to boost the content of larger pro-Chinese accounts or attack opponents online.[8]

Microsoft detected that China's state-affiliated social media influencer initiative successfully engaged target audiences in at least 40 languages with a total audience of more than 103 million people. Campaigns criticizing the United States and other democracies recently expanded into new language platforms including Croatian, Dutch, French, German, Greek, Indonesian, Italian, Norwegian, Slovak, Spanish, Swedish, Thai, Turkish, and Uyghur. After a Spanish human rights organization exposed Chinese police stations operating covertly in foreign countries, Beijing targeted the group with more than 1,800 accounts across several social media platforms and dozens of websites.[9]

While initial Chinese influence and disinformation campaigns were often rudimentary, Microsoft warned that Beijing has honed new capabilities and is now employing more sophisticated techniques, including artificial intelligence (AI). The company assessed that Beijing is now producing high-quality disinformation content and has become more effective at engaging social media users while using fictitious or stolen identities to conceal its Chinese origin.[10]

China's Global Influence Operations

China has implemented covert influence campaigns around the world, most notably targeting Australia, Canada, Hong Kong dissidents, Southeast Asian nations, Taiwan, and the United States.

In Australia, Beijing-linked donors paid prominent politicians to influence Australian foreign policy more favorably toward China.[11] The Australian Secret Intelligence Service subsequently prevented China from providing funds to Australian candidates to support the interests of a foreign government.[12]

In 2023, the Canadian government declared that it had detected a Chinese "Spamouflage" campaign that placed thousands of comments on the Facebook and X/Twitter accounts of dozens of members of parliament. Targeted politicians included the prime minister, the leader of the Official Opposition, and several members of the cabinet. The messages, including disinformation and "deepfake" videos, accused the politicians of criminal and ethical violations.[13]

In 2019, China undertook a targeted disinformation campaign against the Hong Kong protests. Meta (which owns Facebook and Instagram) removed Chinese government–affiliated accounts that used deceptions such as posing as news organizations.[14] The fake accounts posted content that exaggerated protesters' violence in an apparent effort to undermine popular support for the movement.[15]

That same year, Twitter disclosed and disabled 936 China-originated accounts that were part of a government information operation "deliberately and specifically attempting to sow political discord in Hong Kong, including undermining the legitimacy and political positions of the protest movement on the ground." Those accounts were the most active of a larger network of 200,000 accounts.[16]

Overall, nearly 375,000 inauthentic accounts on Twitter, Facebook, and YouTube were attributed to China and involved in the campaign related to Hong Kong.[17] Twitter published more than 3.5 million tweets posted by assets linked to China.[18]

Electoral Interference. Beijing has intervened in elections around the world through coordinated information and disinformation campaigns designed to promote candidates sympathetic to the Chinese government and its actions. Official Chinese statements advocate "political participation by Chinese people" in other countries' elections. Beijing sought to mobilize Chinese diaspora voters to support pro-China candidates and policies, or to attack politicians deemed to be "anti-China."[19] China sought to covertly alter the outcome of elections throughout Southeast Asia through cyber activities and financial donations.[20]

The most notable example was during the 2020 Taiwanese presidential election when China directed Taiwanese media organizations to promote Beijing's favored candidate, Han Kuo-yu.[21] Beijing also spread disinformation to defame President Tsai Ing-wen, including claims of voter fraud. The Chinese government used "content farms" to produce extensive false information articles and recruited Taiwanese social media influencers to push pro-China themes.[22]

In 2020, Twitter removed more than 23,000 accounts for being part of Chinese disinformation campaigns. Themes from the banned accounts had been amplified by an additional 150,000 accounts.[23]

China has sought to influence opinion and the political environment in the United States by targeting politicians seen as "anti-China," sowing discord, anger, and distrust amongst the populace, and interfering with elections. Reports indicate China spent $280 million over a six-year period to influence U.S. politics.[24]

The FBI reported that Chinese hackers employed disinformation and other tactics to interfere in the 2016 and 2018 U.S. elections, though more to sow turmoil rather than push for specific candidates.[25] In 2021, the U.S. Intelligence Community assessed that Beijing had sought to "shape the political environment in the United States to promote [Chinese] policy preferences, mold public discourse, pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China."[26]

Prior to the 2022 U.S. midterm elections, Microsoft identified CCP-affiliated social media accounts impersonating U.S. voters, targeting specific candidates, and responding to comments from authentic users in order to create controversy along racial, economic, and ideological lines.[27]

In 2023, the Department of Justice charged 34 Chinese officials of the Ministry of Public Security (MPS) for running a disinformation operation that utilized hundreds of MPS officers stationed in the U.S. to target critics and dissidents.[28] Mandiant, an American cybersecurity firm, identified a Chinese influence campaign designated "Dragonbridge" that sought to strain relations between the U.S. and its allies by impersonating cyber actors, plagiarizing and altering news articles, and posing as Americans to promote political themes.[29] Twitter identified 2,000 China-based accounts that had issued more than 250,000 tweets containing false election-rigging claims about the 2020 U.S. presidential election.[30]

In 2023, Meta deactivated Chinese-linked fake accounts in what it described as "the largest known cross-platform covert influence operation in the world." The network targeted many regions around the world, including Australia, Japan, Taiwan, the United Kingdom, the United States, and global Chinese-speaking audiences. The operation included 7,704 fake Facebook accounts, 954 fake Facebook pages, and 15 fake groups publishing pro-Chinese talking points and attacking critics. The Chinese influence operation targeted at least 50 other platforms and apps, including Blogspot, Facebook, Instagram, LiveJournal, Medium, Pinterest, Reddit, TikTok, Vimeo, X (formerly Twitter), YouTube, and dozens of smaller platforms and forums.[31]

China Targets South Korea

China has already used several methods to influence South Korean public opinion and policy, including disinformation campaigns, Confucius Institutes, and covert Chinese police stations.

Disinformation Campaigns. President Yoon warned that "rapidly increasing disinformation can undermine our freedom and threaten

democratic systems such as elections." In 2020, the Seoul Central District Prosecutor's Office launched an investigation into allegations that Chinese agents influenced public opinion through manipulation of online communities and comments on portal sites.[32]

In 2023, the South Korean National Intelligence Service disclosed that China sought to manipulate online public opinion and aggravate social divisions by surreptitiously issuing anti-government and pro-China content. Chinese organizations posed as South Korean media companies and created 38 fake news sites to publish articles that criticized the United States, exaggerated dangers from Japan's release of contaminated water from the Fukushima nuclear reactor, and extolled China's response to the COVID-19 pandemic. The sites also disseminated CCP propaganda materials and depicted them as press releases.[33]

To disguise themselves, the organizations adopted media and domain names similar to those of legitimate Korean news agencies and pretended to be members of the Korea Digital News Association. They posted some real Korean news articles to appear as legitimate media.

One of those Chinese organizations also placed pro-Beijing stories on the websites of at least 32 American news outlets, including the *Arizona Republic* and *Pittsburgh Post-Gazette*. The articles included scathing critiques of U.S. policymakers, academics, and others who were critical of Beijing.[34]

Confucius Institutes. Since 2004, China has established government-funded Confucius Institutes in 23 South Korean universities, four high schools, and one private academy, the largest number in any Asian country.[35] While ostensibly providing Chinese language and culture classes, establishing scholarships, academic programs, and exchange programs, the institutes have been credibly accused of exerting control over academic host organizations and conducting influence operations.

Human Rights Watch concluded that Confucius Institutes are extensions of the Chinese government that pressure host universities to censor topics and perspectives in course materials that are deemed to be anti-China and to use hiring practices prioritizing political loyalty.[36] The institutes have tried to shut down events at their host university that were perceived to be hostile to China.[37]

The U.S. government assessed that Confucius Institutes in the United States conduct espionage activities and monitor Chinese students as well as Chinese-Americans involved in human rights activities in the United States.[38] Some Members of the U.S. Congress allege that Confucius Institutes seek to influence public opinion abroad, recruit "influence agents" on U.S. campuses, pressure universities against statements or events sensitive to China, and engage in cyber espionage.[39]

In response, at least 92 universities, two government agencies, and three education committees from around the world have cut ties with Confucius Institutes.[40] More than two-thirds of the Confucius Institutes in the United States have shut down. European countries, including Belgium and the United Kingdom, are closing their Confucius Institutes and there have been calls in Australia to take similar action.[41]

In South Korea, Confucius Institutes led "hostile activities" targeting rallies supporting the Hong Kong democracy movement. A National Assembly member cited a South Korean intelligence report that the institutes mobilized Chinese students to stage counter-protests, defaced pro-democracy posters, and distributed pro-China propaganda at universities in South Korea.[42]

The U.S. Director of National Intelligence has commented that Beijing monitors overseas Chinese students for dissident views and mobilizes Chinese student associations to conduct activities on behalf of Beijing and pressure family members in China to stifle anti-Beijing criticism.[43] The Korea Defense Network declared that Chinese agents were suspected of using Chinese migrant workers and students in South Korea to influence South Korean public opinion online in favor of China.[44]

Covert Chinese Police Stations. As it has in other countries, China established covert police stations in South Korea to monitor and intimidate Chinese citizens. South Korean authorities investigated reports of at least four undeclared Chinese police stations—two in Seoul and two on Jeju Island.[45]

Safeguard Defenders, an international human rights group, identified 102 Chinese police stations in 53 countries. The group reported that the CCP's United Front Work Department oversees the police stations whose main function is to pressure dissidents to return to China to face criminal charges. Chinese police and security personnel routinely conduct such illegal operations in other countries.[46]

Since 2014, China has engaged in a repression program designated Operation Fox Hunt (incorporated into Operation Sky Net in 2015) to forcibly repatriate overseas Chinese "fugitives." Chinese police officers working illegally in the target country may threaten the target's family still in China with arrest or other punitive actions if the fugitive does not return to China. Other methods include coercing the target directly or kidnapping and forced repatriation to China. Sometimes targets are given the choice to accept deportation to China or stay in the host country to spy on other Chinese nationals there.[47]

Beijing claims that more than 10,000 people have been repatriated to China from more than 120 countries under Operation Fox Hunt/Sky Net. Very few of these were processed legally. Chinese state media reported that 1,273 fugitives were returned to China in 2021 alone without repercussions.[48]

Electoral System Vulnerabilities. South Korea's National Intelligence Agency and the Korea Internet and Security Agency have both warned that the voting and ballot counting systems of the National Election Commission (NEC) remain vulnerable to hacking by Chinese actors. A government probe revealed multiple cybersecurity vulnerabilities of the NEC voter register, ballot counting, and early voting systems, which would enable hackers to penetrate the network and manipulate registered voter information and the outcome of an election.[49]

South Korea Considers Responses. The South Korean National Assembly has debated legislative measures to augment existing law enforcement authorities against influence operations. Representative Choi Jae-hyung from the ruling People Party Power introduced a bill that would require all foreign government agents to register with the Justice Ministry. Choi stated that doing so would enable authorities to more easily detect foreign operations for influencing public opinion or government policies.[50]

Other proposed legislation would expand current espionage laws beyond threats from North Korea. Current South Korea law is narrowly restricted to national security threats that solely benefit "the enemy state," meaning North Korea. Activities on behalf of other nations, including China, cannot be prosecuted under the existing law.[51]

In September 2023, the Korea Communications Commission (KCC) announced that it would launch a task force to eradicate fake news, which it cited as having caused damage, including influencing results of major elections. The KCC will seek to introduce a "one-strike-out system" whereby media outlets will be immediately expelled if they are found to have released even a single fake malicious report. The task force will also recommend new rules for social media sites.[52]

In October 2023, the ruling People Power Party (PPP) proposed legislation to prevent foreign manipulation of online opinions in South Korea. The initiative is a response to a KCC emergency report that foreign agents had used virtual private networks to appear as Korean residents to generate large numbers of pro-China comments on websites of South Korea's second-largest online portal.[53]

Representative Park Sung-joong accused China of influence operations and advocated legislative action targeting perpetrators, accomplices, and web portal companies that fail to respond. Park warned that China or North Korea could seek to influence the April 2024 National Assembly elections through disinformation campaigns against certain candidates to help to elect their competitors.[54]

In October 2023, Prime Minister Han Duck-soo ordered South Korea's cabinet to set up a governmental task force to prevent "fake news" from manipulating public opinion. He warned that "fake news is a serious social disaster that shakes the foundation of democracy."[55]

Influencing South Korean Elections

As it has in other countries, China could seek to influence South Korean elections by exploiting the fierce partisan differences between conservatives and progressives (referred to as the "south-south divide"). Beijing could do so by developing new narratives or by affirming and amplifying existing grievances, such as anti-American and anti-Japanese emotions, which are strongest amongst progressives, as well as playing to fears of triggering Chinese economic retaliation.

The Chinese goal would be to raise criticism and resistance to President Yoon's policies in order to help the progressive Democratic Party of Korea (DPK) do better in the elections which, in turn, would hinder Yoon's ability to continue his principled policies. The opposition DPK is more accommodating to North Korea and China and seeks to distance itself from the United States. The party currently has a majority in the unicameral National Assembly and adding to its ranks in the election would further embolden obstruction to Yoon's policy and budget requests.

Recommendations for South Korea

Given the extent and potential impact of Chinese covert influence operations, the United States should closely coordinate with its key regional ally to prevent China from covertly swaying South Korean policies away from those in Washington's strategic interests. This initiative could then serve as a model for other American allies who are targeted by these disinformation campaigns.

Seoul should implement a multifaceted strategy to reduce Beijing's efforts to effect South Korean public opinion, government policies, and election results. The South Korean government should:

Assess the Threat. South Korea should initiate a comprehensive investigation to determine the characteristics and scope of current Chinese influence operations as well as the potential capabilities of future campaigns. Seoul should identify Chinese coercive activity objectives, likely themes for exploitation, potential instruments for implementation, and South Korean vulnerabilities. The investigation should include a review of

past and ongoing Chinese operations and tactics not only in South Korea but also of those directed against other countries, most notably Australia, Canada, Taiwan, and the United States. South Korea should augment its research by consulting with outside experts, social media companies, and computer security firms.

Develop a Comprehensive Strategy and Create a Policy Coordinator. Addressing China's influence operations should be a national priority that requires a comprehensive whole-of-government response in conjunction with private-sector partners. Seoul should identify a lead agency or coordinator to direct, synchronize, and coordinate the implementation of a new strategy and engage with private-sector and foreign government partners.

Coordinate Policies with Domestic and International Partners. South Korea should mobilize a consortium of public-sector and private-sector actors to collectively counter Chinese influence and disinformation operations. Seoul should begin with domestic entities and then build an international network of partners to enhance vigilance and cooperation against a common threat. Participants should include government agencies; law enforcement agencies; social media, technology, and computer security companies; print, radio, and TV media firms; academic institutions; think tanks; and civil society organizations.

The international consortium could share information on Chinese influence operations, best practice responses, and recommended technology, training, defense enhancements, and countermeasures. European partners could provide information on lessons learned from combating similar Russian disinformation and influence operations.

Cyber operations are one component of the overall Chinese influence campaign. As such, international cross-sectoral coordination could piggyback on ongoing cybersecurity initiatives. South Korea is currently engaged with numerous international entities countering Chinese and North Korean cyber-threats. South Korea has also pledged greater cybersecurity cooperation with the United States and Japan in the August 2023 Camp David Accord and with the United Kingdom in the November 2023 Downing Street Accord. In December 2023, South Korea signed a memorandum of understanding with the United States to jointly tackle foreign disinformation.[56]

However, both South Korean and international efforts must not use fear of the potential impact of foreign disinformation to constrain constitutionally protected freedom of expression or censor citizens' criticism of their government or its policies. Public-sector and private-sector initiatives must be solely directed against Chinese-initiated foreign influence operations.

Work with Social Media Companies to Enhance Protection Against Disinformation. Seoul should encourage discussions and exchange of research between South Korea–based social media companies with their U.S. counterparts (Facebook, Instagram, Twitter/X, and YouTube) to enhance attribution of foreign influence–driven disinformation on their platforms.

To promote a more transparent and open media environment, South Korea should assess the need for social media companies and Internet providers to implement additional measures to detect disinformation, identify state-affiliated and proxy media accounts, and provide greater transparency of social media algorithms.

Expose and Publicize Chinese Illicit Influence Operations. South Korea should disclose China's covert influence campaign by publicly detailing objectives, targets, tactics, techniques, and facilitators. To the extent possible, Seoul should declassify intelligence information to increase public trust in the government's conclusions of Chinese interference in South Korean affairs.

The government should issue threat advisories detailing the extent of Beijing's covert efforts against academic institutions, think tanks, social media sites, print and television media, and the government. Being more cognizant of the threat enables those institutions and the general public to reduce exposure, increase resistance and protection measures, and more effectively combat Beijing's disinformation operations.

South Korea should make clear that it will continue to expose and respond to Chinese improprieties. President Yoon has emphasized that he expects bilateral relations with Beijing to be based on principals of non-interference and mutual respect, which is impossible under current circumstances.

Fully Enforce Existing Laws Against Influence Operations, Disinformation, and Electoral Interference. Seoul should take action against any actors engaged in or facilitating Chinese illicit activities affecting South Korean media, public opinion, or elections. The government should coordinate the collaboration amongst regulatory agencies, financial oversight entities, and law enforcement entities. Social media companies, Internet service providers, and telecommunications firms should be required to exercise due diligence against covert activities and identify foreign government propaganda.

Respond Rapidly and Forcefully to Illicit Influence Operations. Seoul should create a government task force to quickly react and identify foreign disinformation and influence campaigns. The identities of perpetrators, along with any foreign government sponsorship, should also be publicized.

Shut Down Confucius Institutes and Illegal Chinese Police Stations. Following the precedent of other nations, South Korea should disband all Chinese government–funded organizations that spread Chinese propaganda and disinformation, curtail academic freedom, constrain intellectual debate, and engage in illicit law enforcement and coercive actions against Chinese nationals in South Korea. Academic institutions should be required to report foreign funding, grants, and gifts.

Seoul should investigate whether any occurrences of Chinese illegal forcible repatriations of Chinese nationals under Operations Fox Hunt/Sky Net have occurred in South Korea. Seoul should take all necessary action to prevent such operations from taking place and make clear to Beijing that such violations of Korean sovereignty will not be tolerated.

Evaluate the Need for Additional Legislation and Regulations. South Korea should determine whether the existing framework of regulations and laws is sufficient for:

- Disclosure of financial relationships (ownership, investment, and funding) of South Korean entities that may be subject to foreign influence;
- Transparency of actions taken by foreign agents acting in South Korea;
- Strength of espionage laws to penalize foreign actors or domestic facilitators that are disseminating disinformation, conducting influence operations, election interference, and cyberattacks; and
- Oversight of social media platforms to ensure removal of false information.

However, any additional enhanced legislation must be weighed carefully against the potential for excessive government constraints on civil liberties. South Koreans well remember the country's authoritarian past and abuses against freedoms of speech and the press. Seoul must be careful to not intervene too much with traditional and social media lest it jeopardize the institutions it is seeking to protect.

Successive South Korean administrations have received criticism for targeting the media in response to articles critical of the standing president. Additional authorities for monitoring against influence operations could be used for censorship.

Conclusion

Chinese covert influence and disinformation operations are a threat to South Korean liberal democracy and U.S. strategic interests in the Indo–Pacific. Beijing seeks to manipulate public opinion, erode public confidence in democratic institutions, divide America's allies, and undermine resistance to China's intimidating and expansionist policies. The growth of AI and other technologies will make foreign influence operations even more effective and difficult to detect.

Targeting Chinese disinformation campaigns in South Korea can be the foundation of a larger effort to counteract this problem globally. The United States should work closely with its critical South Korean ally and other partners to augment defenses against Chinese covert activities and respond forcefully to disinformation campaigns and other influence operations. Failure to do so weakens international efforts to uphold democratic principles, protect its citizenry, and prevent encroachment on national sovereignty.

Bruce Klingner is Senior Research Fellow for Northeast Asia in the Asian Studies Center at The Heritage Foundation.

Endnotes

1. National Bureau of Asian Research, "Understanding Chinese 'Wolf Warrior Diplomacy,'" October 22, 2021, https://www.nbr.org/publication/understanding-chinese-wolf-warrior-diplomacy/ (accessed February 13, 2024).
2. Malcolm Turnbull, "Speech Introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017," December 7, 2017, https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an (accessed December 13, 2023).
3. U.S. Department of State Global Engagement Center, "How the People's Republic of China Seeks to Reshape the Global Information Environment," *Special Report*, September 2023, https://www.state.gov/wp-content/uploads/2023/09/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_Final.pdf (accessed December 13, 2023).
4. Patrick Wintour, "China Spends Billions on Pro-Russia Disinformation, US Special Envoy Says," *The Guardian*, February 28, 2023, https://www.theguardian.com/world/2023/feb/28/china-spends-billions-on-pro-russia-disinformation-us-special-envoy-says (accessed December 13, 2023).
5. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf (accessed December 13, 2023).
6. James Kynge, Lucy Hornby, and Jamil Anderlini, "Inside China's Secret 'Magic Weapon' for Worldwide Influence," October 26, 2017, https://www.ft.com/content/fb2b3934-b004-11e7-beba-5521c713abf4 (accessed December 13, 2023).
7. U.S. Department of State Global Engagement Center, "How the People's Republic of China Seeks to Reshape the Global Information Environment."
8. International Republican Institute, "Countering China's Information Manipulation: A Toolkit for Understanding and Action," September 6, 2023, https://www.iri.org/resources/countering-chinas-information-manipulation-a-toolkit-for-understanding-and-action/ (accessed December 13, 2023).
9. Microsoft, "Digital Threats from East Asia Increase in Breadth and Effectiveness," September 2023, https://www.microsoft.com/en-us/security/business/security-insider/reports/nation-state-reports/digital-threats-from-east-asia-increase-in-breadth-and-effectiveness/ (accessed December 13, 2023).
10. Ibid.
11. Amy Remeikis, "Sam Dastyari Quits as Labor Senator Over China Connections," *The Guardian*, December 11, 2017, https://www.theguardian.com/australia-news/2017/dec/12/sam-dastyari-quits-labor-senator-china-connections (accessed December 13, 2023).
12. "Chinese Political Interference Has Western Spooks Worried," *The Economist*, April 21, 2022, https://www.economist.com/china/2022/04/21/chinese-political-interference-has-western-spooks-worried (accessed December 13, 2023).
13. Government of Canada, "Rapid Response Mechanism Canada Detects Spamouflage Campaign Targeting Members of Parliament," October 23, 2023, https://www.canada.ca/en/global-affairs/news/2023/10/rapid-response-mechanism-canada-detects-spamouflage-campaign-targeting-members-of-parliament.html (accessed December 13, 2023).
14. Meta, "Removing Coordinated Inauthentic Behavior from China," August 19, 2019, https://about.fb.com/news/2019/08/removing-cib-china (accessed December 13, 2023).
15. Heidi Holz and Anthony Miller, "China's Playbook for Shaping the Global Media Environment," Center for Naval Analyses, February 2020, https://www.cna.org/reports/2020/02/IRM-2020-U-024710-Final.pdf (accessed December 13, 2023).
16. X (formerly Twitter), "Information Operations Directed at Hong Kong," August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong (accessed December 13, 2023).
17. Renée Diresta et al., "Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives," Standford Internet Observatory and Hoover Institution, 2020, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf (accessed December 13, 2023).
18. Ben Nimmo, C. Shawn Eib, and L. Tamora, "Cross-Platform Spam Network Targeted Hong Kong Protests," Graphika, September 2019, https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf (accessed December 13, 2023).
19. International Republican Institute, "Countering China's Information Manipulation: A Toolkit for Understanding and Action."
20. Abby Seiff, "Chinese State-Linked Hackers Target the Cambodian Elections," *Time*, July 10, 2018, https://time.com/5334262/chinese-hackers-cambodia-elections-report/ (accessed February 13, 2024), and Tom Wright and Bradley Hope, "WSJ Investigation: China Offered to Bail Out Troubled Malaysian Fund in Return for Deals," *The Wall Street Journal*, January 7, 2019, https://www.wsj.com/articles/how-china-flexes-its-political-muscle-to-expand-power-overseas-11546890449 (accessed December 13, 2023).
21. Joshua Kurlantzick, "China's Growing Attempts to Influence U.S. Politics," Council on Foreign Relations, October 31, 2022, https://www.cfr.org/ /chinas-growing-attempts-influence-us-politics (accessed December 13, 2023).
22. Jude Blanchette et al., "Protecting Democracy in an Age of Disinformation," Center for Strategic and International Studies, January 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210127_Blanchette_Age_Disinformation.pdf (accessed December 13, 2023).

23. Kenddrick Chan and Mariah Thornton, "China's Changing Disinformation and Propaganda Targeting Taiwan," *The Diplomat*, September 19, 2022, https://thediplomat.com/2022/09/chinas-changing-disinformation-and-propaganda-targeting-taiwan/ (accessed December 13, 2023).
24. Kurlantzick, "China's Growing Attempts to Influence U.S. Politics."
25. "China, Caught Meddling in Past Two US Elections, Claims 'Not Interested' in 2020 Vote," Voice of America, April 30, 2020, https://www.voanews.com/a/east-asia-pacific_china-caught-meddling-past-two-us-elections-claims-not-interested-2020-vote/6188474.html (accessed December 13, 2023).
26. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf (accessed December 13, 2023).
27. Microsoft, "Digital Threats from East Asia Increase in Breadth and Effectiveness."
28. Donie O'Sullivan, Curt Devine, and Allison Gordon, "China Is Using the World's Largest Known Online Disinformation Operation to Harass Americans, a CNN Review Finds," CNN, November 13, 2023, https://www.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html (accessed December 13, 2023).
29. Mandiant, "New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections," October 26, 2022, https://www.mandiant.com/resources/blog/prc-dragonbridge-influence-elections (accessed December 13, 2023).
30. Craig Singleton, "Chinese Election Meddling Hits the Midterms," *Foreign Policy*, November 4, 2022, https://foreignpolicy.com/2022/11/04/china-us-midterm-election-interference-meddling-social-media-cybersecurity-disinformation/ (accessed December 13, 2023).
31. Ben Nimmo et al., "Second Quarter Adversarial Threat Report," Meta, August 2023, https://about.fb.com/news/2023/08/raising-online-defenses/ (accessed December 13, 2023).
32. Korea Broadcasting System, "Prosecutors Begin Investigation Into 'Chinagate' Accusation Case," March 11, 2020, in Korean, translated with Google Translate, https://news.kbs.co.kr/news/pc/view/view.do?ncd=4399281&ref=A (accessed December 13, 2023).
33. Tara O, "China's 38 Fake News Sites Disseminating Pro-China, Anti-US, Anti-Japan Content in South Korea," East Asia Research Center, November 18, 2023, https://eastasiaresearch.org/2023/11/18/chinas-38-fake-news-sites-disseminating-pro-china-anti-us-anti-japan-content-in-south-korea/?amp=1&utm (accessed February 13, 2024), and Ryan Serabian and Daniel Kapellmann Zafra, "Pro-PRC 'HaiEnergy' Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites," Mandiant, August 4, 2022, https://www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy (accessed December 13, 2023).
34. Cate Cadell and Tim Starks, "Pro-China Influence Campaign Infiltrates U.S. News Websites," *The Washington Post*, July 24, 2023, https://www.washingtonpost.com/politics/2023/07/24/pro-china-influence-campaign-infiltrates-us-news-websites/ (accessed February 13, 2024), and Ryan Serabian et al., "Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C.," Mandiant, July 24, 2023, https://www.mandiant.com/resources/blog/pro-prc-haienergy-us-news#:~:text=This%20campaign%2C%20which%20we%20dubbed,strategically%20aligned%20with%20the%20political (accessed December 13, 2023).
35. "'In the Name of Confucious' Korea Premiere Revealing the Reality of the Confucius Institute—The Epoch Times (South Korea)," In the Name of Confucius, May 22, 2021, https://inthenameofconfuciusmovie.com/in-the-name-of-confucius-korea-premiere-revealing-the-reality-of-the-confucius-institute-the-epoch-times-south-korea/ (accessed December 13, 2023).
36. Human Right Watch, *World Report 2019*, https://www.hrw.org/world-report/2019/country-chapters/china (accessed December 13, 2023).
37. Bethany Allen-Ebrahimian, "How China Managed to Play Censor at a Conference on U.S. Soil," *Foreign Policy*, May 9, 2018, https://foreignpolicy.com/2018/05/09/how-china-managed-to-play-censor-at-a-conference-on-u-s-soil/ (accessed December 13, 2023).
38. "'In the Name of Confucius' Korea Premiere Revealing the Reality of the Confucius Institute—The Epoch Times (South Korea)," In the Name of Confucius.
39. Thomas Lum and Hannah Fischer, "Confucius Institutes in the United States: Selected Issues," Congressional Research Service, May 2, 2023, https://crsreports.congress.gov/product/pdf/IF/IF11180 (accessed December 13, 2023).
40. "'In the Name of Confucius' Korea Premiere Revealing the Reality of the Confucius Institute—The Epoch Times (South Korea), In the Name of Confucius.
41. "Confucius Institutes Grow Deeper Roots in South Korea," One Korea Network, September 26, 2021, https://onekoreanetwork.com/2021/09/26/confucius-institutes-grow-deeper-roots-in-south-korea/ (accessed December 13, 2023).
42. Kim Arin, "China-Sponsored Confucius Institutes Behind 'Hostile Activities' Against Pro-Hong Kong Rallies in Seoul: Lawmaker," *The Korea Herald*, June 15, 2023, https://www.koreaherald.com/view.php?ud=20230615000763 (accessed February 13, 2024), and Kim Arin, "Nationwide Probe Launched Into Secret Chinese 'Police Stations' in South Korea," *The Korea Herald*, June 16, 2023, https://www.koreaherald.com/view.php?ud=20230616000517 (accessed December 13, 2023).
43. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023.
44. Park Chan-kyong, "South Korea Investigates Secret Chinese 'Police Stations' After Claims of 2 More Being Uncovered on Jeju Island," *South China Morning Post*, June 20, 2023, https://www.scmp.com/week-asia/people/article/3224646/south-korea-investigates-secret-chinese-police-stations-after-claims-2-more-being-uncovered-jeju (accessed December 13, 2023).

45. Chung Yeong-gyo, "Suspected Secret Chinese Police Base Has Another Branch Near Seoul's National Assembly," *Korea Joongang Daily*, December 26, 2022, https://koreajoongangdaily.joins.com/2022/12/26/national/diplomacy/korea-china-china-secret-police/20221226115529236.html (accessed February 13, 2024), and Park, "South Korea Investigates Secret Chinese 'Police Stations' After Claims of 2 More Being Uncovered on Jeju Island."
46. Safeguard Defenders, "Patrol and Persuade: A Follow-up Investigation to 110 Overseas," 2022, https://safeguarddefenders.com/sites/default/files/pdf/Patrol%20and%20Persuade%20v2.pdf (accessed December 12, 2023).
47. Safeguard Defenders, "Involuntary Returns: China's Covert Operation to Force 'Fugitives' Overseas Back Home," 2022, https://safeguarddefenders.com/sites/default/files/pdf/INvoluntary%20Returns.pdf (accessed December 13, 2023).
48. Michael Cunningham, "Chinese Spies Violate U.S. Sovereignty and Americans' Rights," *The Wall Street Journal*, May 6, 2022, https://www.wsj.com/articles/chinese-spies-violate-u-s-sovereignty-and-americans-rights-operation-sky-net-xi-illegal-victim-repatriated-smuggle-human-rights-11651848282 (accessed December 14, 2023).
49. Kim Soo-yeon, "Election Watchdog's Cybersecurity System Vulnerable to Hacking Attacks: NIS," Yonhap, October 10, 2023, https://en.yna.co.kr/view/AEN20231010004001315 (accessed December 13, 2023).
50. Park, "South Korea Investigates Secret Chinese 'Police Stations' After Claims of 2 More Being Uncovered on Jeju Island."
51. Lee Jeong-Ho, "Suspected Covert Chinese Outpost Sparks Push for S. Korea 'Spy Bill,'" Radio Free Asia, September 19, 2019, https://www.rfa.org/english/news/china/korea-chinese-spying-09192023035249.html (accessed December 13, 2023).
52. KBS World, "KCC to Launch Task Force on Stamping out Fake News," September 6, 2023, https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=180304 (accessed December 13, 2023).
53. Yoo Cheong-mo, "PM Orders Pan-Gov't Taskforce to Tackle Suspected Opinion Manipulation on Portal Daum," Yonhap, October 4, 2023, https://en.yna.co.kr/view/AEN20231004003551315 (accessed December 13, 2023).
54. Jung Min-ho, "Ruling Party Vows to Investigate China's Alleged Influence Operations," *The Korea Times*, October 3, 2023, https://www.koreatimes.co.kr/www/nation/2023/10/120_360354.html (accessed December 13, 2023).
55. Yoo, "PM Orders Pan-Gov't Taskforce to Tackle Suspected Opinion Manipulation on Portal Daum."
56. Christy Lee, "US Deals with Allies Signal Concerns Over China's Disinformation Campaign," Voice of America, December 8, 2023, https://www.voanews.com/a/us-deals-with-allies-signal-concerns-over-china-s-disinformation-campaign-/7389344.html (accessed December 12, 2023).