DISINFORMATION

Jessica Brandt

Maiko Ichihara

Nuurrianti Jalli

Puma Shen

Aim Sinpeng

OVERVIEW: IMPACT OF DISINFORMATION ON DEMOCRACY IN ASIA

JESSICA BRANDT

THE NATURE OF THE PROBLEM

In Asia and around the world, disinformation campaigns — perpetrated by foreign actors seeking to shore up power at home and weaken their competitors abroad and by domestic actors seeking political advantage — are increasingly putting pressure on democratic societies. This pressure manifests through several pathways.

- Democratic societies rest on the idea that the truth is knowable and that citizens can discern and use it to govern themselves. Because disinformation feeds skepticism that there is such a thing as objective truth, it undermines the very foundation of self-government.[1]
- A frequent tactic of foreign information manipulation campaigns is to amplify the most extreme views within a target society in order to weaken it from within. Meanwhile, domestic purveyors of disinformation often seek to demonize political opponents for electoral advantage. As a result, disinformation frequently drives polarization, making it harder for democratic societies to govern themselves.

Illiberal governments in particular use information manipulation campaigns to dampen the appeal of democracy. This is especially the case for Beijing-backed information operations targeting democratic societies in Asia. By making democracy less attractive to would-be rights activists, autocrats hope to tighten their grip on power at home.[2] But these activities can also depress support for democracy within target societies.

Autocrats generally, and Chinese President Xi Jinping specifically, use these campaigns to broadly undermine liberal norms such as respect for human and political rights, including rights to privacy and expression. This is primarily to create a more enabling environment for Beijing's illiberal practices at home, but it can have detrimental effects on the rights and freedoms of citizens beyond its borders, even in Asia's consolidated democracies.

Meanwhile, disinformation spread by domestic political actors can further erode trust, and perhaps ultimately participation, in democratic institutions. It can also lead to intracommunal violence.[3]

SCOPE OF THE CHALLENGE IN ASIA

In Japan, as elsewhere, natural disasters and elections have been flashpoints for the spread of information that is false or misleading. Maiko Ichihara documents the spread of Russian propaganda in Japan about Moscow's invasion of Ukraine, and how these narratives are proliferated by Russian diplomats, domestic conspiracy theorists, and accounts that regularly amplify Chinese government content. Her findings highlight the extent to which foreign and domestic information operations are intertwined, as is the case across many other contexts.

In Malaysia, a combination of actors, often domestic, propagate disinformation in multiple local languages. Nuurrianti Jalli highlights how coordinated information campaigns surrounding elections in Malaysia have made it

difficult for Malaysian citizens to make informed decisions about candidates and issues and have been used by leaders to gain and maintain power, contributing to democratic backsliding. She also points to the enactment of legislative measures that give government "a vast power to use to 'countering disinformation' to justify restricting freedom of expression," a development in keeping with a worldwide trend.[4]

Taiwan, which has been ranked as the country most targeted by false information since 2013, faces an onslaught of disinformation from China.[5] Puma Shen illustrates how the Chinese government uses disinformation in combination with other tools — including nontransparent funding and personal ties — to extend its influence. He also highlights Beijing's efforts to use authentic Taiwanese voices to make its information campaigns more difficult to identify and counter. China deploys such strategies all around the world.[6] As Shen observes, the Taiwanese government implemented a Disinformation Coordination Team in 2018, but although it has been quite effective in some cases, several of its efforts have exposed the limits of government-led (vs. civil society) activity in the information domain.

Thailand, which has had an illiberal internet environment for almost a decade according to multiple watchdog groups, remains a surprisingly vibrant hub of digital activism — offering hope for democratic resilience in the face of disinformation and digital repression.[7] Aim Sinpeng documents three key drivers of disinformation in Thailand: the campaigns of domestic political leaders that seek to attack opposition groups and shape public perceptions of government institutions; the growing influence of China in Thailand's traditional media and technology landscapes; and the existence of a legal framework that gives state agencies power to exert control over information.

RECOMMENDATIONS FOR COUNTERING DISINFORMATION IN ASIA

A number of recommendations for governments, civil society leaders, and social media platforms emerge from these country assessments. Building resilience to and countering manipulative information campaigns is a whole-of-society endeavor.

- Recognizing limits on what government can do in the information space, civil society should play a prominent role in combatting disinformation in Asia. To this end, universities should facilitate the sharing of data and analysis software among trusted researchers. Nongovernmental organizations should build resilience to disinformation by working to improve media literacy. Philanthropists should invest in projects that support the study of emerging good practices in Asian contexts and foster vibrant, independent, investigative media. Because civil society leaders are often targets of disinformation campaigns, special attention should be paid to providing them with resources and training to strengthen their capacity to conduct their work.

- Recognizing that foreign information manipulation is a national security challenge, affected governments should expand resources devoted to disinformation analysis. Working together with civil society researchers, policymakers should raise the level of awareness of these disinformation campaigns by exposing them and sharing examples publicly. Civil society organizations could use social technologies, like games or other apps, to raise awareness of the challenge.

- Policymakers in countries like Taiwan, where the Chinese government uses opaque investments as a tool of influence, should establish policies that promote greater financial transparency.

- Major social media platforms operating in Asia should dedicate additional resources to content moderation in local languages. The platforms should collaborate where possible and appropriate with democratic governments operating under rule of law principles and be wary of collaboration with those governments that are less than wholly free so as not to become an instrument of repression. With that in mind, platforms should be more transparent about the

content moderation requests they receive from state actors, how they respond to those requests, and on what basis.

- Democratic governments should be aware that the measures they adopt to address disinformation at home may be used to justify rights restrictions in less free environments. This should not stop democratic governments from legislating entirely, but it should inform their thinking.
- Democratic governments and civil society actors in Asia and around the world should share lessons learned and exchange examples of good practice. This could take place through formal channels and through informal networks of researchers and activists facing similar challenges.

REFERENCES

1 Jessica Brandt, "How Democracies Can Win an Information Contest Without Undercutting Their Values," Carnegie Endowment for International Peace, August 2, 2021, https://carnegieendowment.org/2021/08/02/how-democracies-can-win-information-contest-without-undercutting-their-values-pub-85058.

2 Jessica Brandt, "How Autocrats Manipulate Online Information: Putin's and Xi's Playbooks," *The Washington Quarterly* 44, no. 3 (September 2021): 127-154, https://www.tandfonline.com/doi/abs/10.1080/0163660X.2021.1970902.

3 For example, in Bangladesh, India, Myanmar, and Sri Lanka. See "The Rise and Digital Authoritarianism: Fake news, data collection and the challenge to democracy," Freedom House, October 31, 2018, https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy.

4 Adrian Shahbaz and Allie Funk, "Freedom on the Net 2021: The Global Drive to Control Big Tech," (Washington, DC: Freedom House, 2021), https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

5 "Varieties of Democracy," https://www.v-dem.net/.

6 Jessica Brandt, book chapter forthcoming.

7 Adrian Shahbaz and Allie Funk, "Freedom on the Net 2021: The Global Drive to Control Big Tech"; "Varieties of Democracy."

HOW TO TACKLE DISINFORMATION IN JAPAN:
LESSONS FROM THE RUSSIA-UKRAINE WAR

MAIKO ICHIHARA

Extensive Russian disinformation and propaganda about the Russia-Ukraine war have been disrupting the discursive space in Japan. The impact of this disinformation is unprecedented in Japan, making this a useful case study for analyzing the disinformation challenge and possible appropriate countermeasures. This paper discusses Japan's disinformation situation in relation to the Russia-Ukraine war, current countermeasures against disinformation, and recommended policies to overcome the challenges.

RUSSIAN DISINFORMATION ABOUT THE AGGRESSION AGAINST UKRAINE

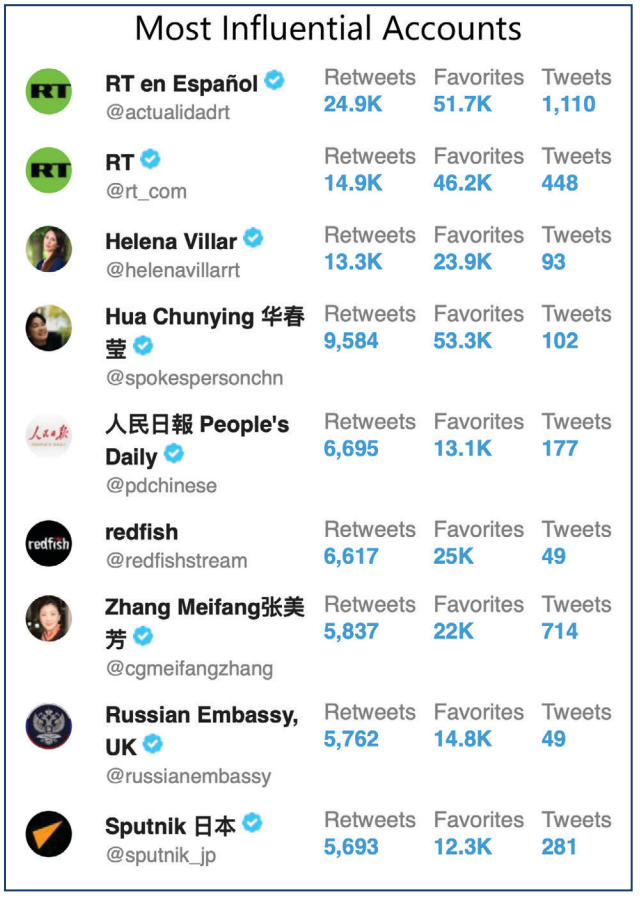
Japan has been considered relatively immune to disinformation, due to the relatively low use of social networking services (SNSs) and the high level of trust in traditional media.[1] But awareness about disinformation and its impact on politics increased in Japan after the flood of disinformation regarding the 2016 U.S. presidential election was discovered. This was also the time when misinformation spread by medical information aggregator sites such as WELQ became a social problem in the country.[2] According to a report by the Study Group on Platform Services, set up by the Ministry of Internal Affairs and Communications, disinformation is disseminated extensively during disasters and elections, in addition to what is spread from aggregator sites during normal times.[3] It is thus natural that studies on disinformation have expanded, with a particular focus on its impact on elections.[4]

What is unexpected is the level of confusion that Russian disinformation about the war with Ukraine has caused in the Japanese discursive space. According to Hamilton 2.0, operated by the German Marshall Fund's Alliance for Securing Democracy, the Twitter account of the Russian embassy in Japan has been consistently ranked the fourth or fifth most influential account among Russian government Twitter accounts around the world since the aggression began (see figure 1). While other top influential accounts are disseminating messages in either Russian as the country's native language, or in languages with large speaker population such as English and Spanish, this embassy account is tweeting in Japanese, a language with a limited number of speakers. The account's performance shows just how effective the approach has been.

The SNS business model of attention economy, which tries to obtain people's attention rather than disseminating preferable information, is helping the voice of the Russian embassy spread within Japanese society. The Russian state media outlet Sputnik also has a Japanese Twitter account, but it does not enjoy much popularity. The reason for the difference seems to be that the Russian embassy account focuses on messages that agitates, while the Sputnik account focuses only on disseminating articles. This contrast can likely be ascribed to a difference in the personalities and approaches of the persons in charge of these Twitter accounts.

FIGURE 1

Most influential Russian accounts on Twitter (as of May 1, 2022)



Source: German Marshall Fund's Alliance for Securing Democracy, Hamilton 2.0 Dashboard, https://securingdemocracy.gmfus.org/hamilton-dashboard/, accessed May 1, 2022.

Tweets spreading Russian disinformation — including claims that the Ukrainian government is neo-Nazi and committing genocide or that the Russian military massacre in the Ukrainian city of Bucha was a fabrication — have been disseminated widely. Some tweets were retweeted over 300 times. According to research conducted by Fujio Toriumi at the University of Tokyo, by March 5, 2022, there were about 10,000 accounts spreading the claim that the Ukrainian government is neo-Nazi.[5]

There are two types of actors spreading Russian propaganda in Japan besides the Russian state media and trolls: conspiracy theorists and pro-Beijing trolls. Japanese newspapers have reported that some of the accounts spreading Russian disinformation now are those that have posted about different conspiracy theories in the past, including from QAnon.[6] Gaining less attention, but still notable, are the accounts that normally support Chinese government propaganda but are now spreading Russian government propaganda and disinformation.

In addition to being influential, however, these disinformation campaigns have increased the Japanese people's awareness about disinformation. Figure 2 shows the number of *Nikkei Shimbun* articles that have contained the term "disinformation." While the number of articles increased after the 2016 U.S. presidential election, it rose further after the COVID-19 pandemic began and then spiked in March 2022 at the start of the Russian hybrid war against Ukraine.

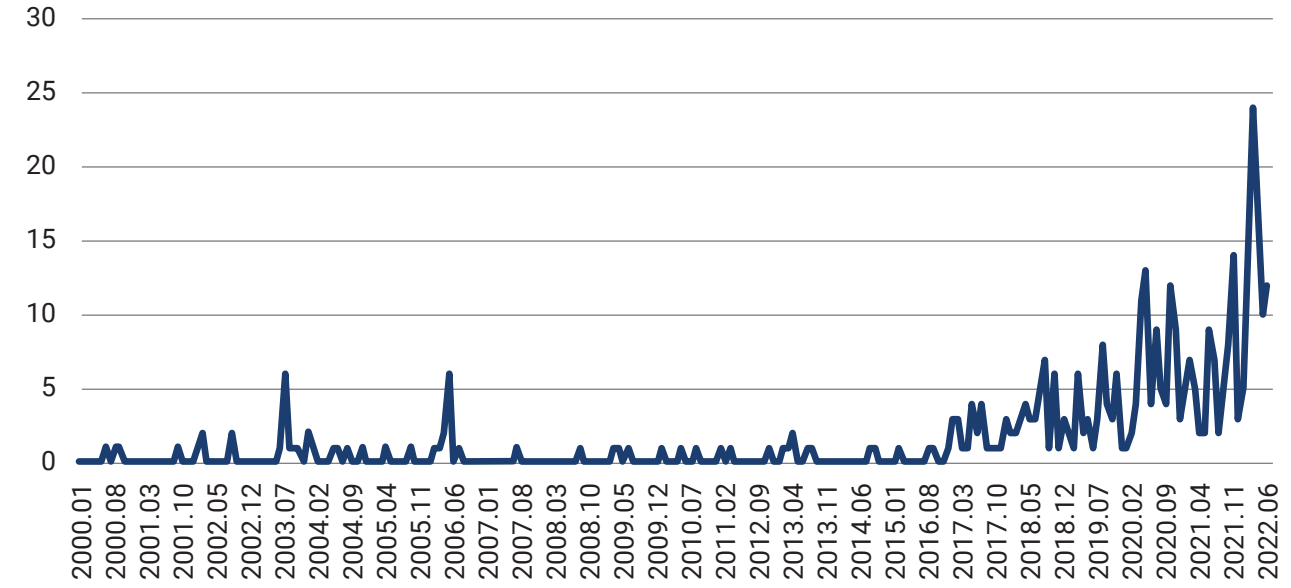
Consequent spread of whataboutism

The proliferation of Russian disinformation and propaganda has not only confused the discourse and created conflict within society but also unintentionally dragged people into the discourse who would not normally be part of disseminating disinformation. In their sincere attempts to pursue justice, Japanese commentators write articles asking whether Russia is really the only one to be blamed, an approach that has been criticized by scholars of international relations for "whataboutism."[7] While these articles state that a violation of sovereignty and the act of aggression are destructive of the international order and do not defend these actions per se, the articles relativize Russia's military violation of international law by considering or suggesting the possibility that Ukraine, the United States, or the West may also have caused the aggression.

Why are these people, who are not trying to be aligned with conspiracy theorists, spreading such messages? To answer this question, this paper outlines the results of an analysis of articles in which whataboutism can be found. The databases of the *Asahi*, *Nikkei*, *Mainichi*, and *Yomiuri Shimbun* newspapers were used to compile the articles, and articles published between January 1, 2021 and May 3, 2022 were searched using "NATO expansion" as the keyword (the explanations used

FIGURE 2

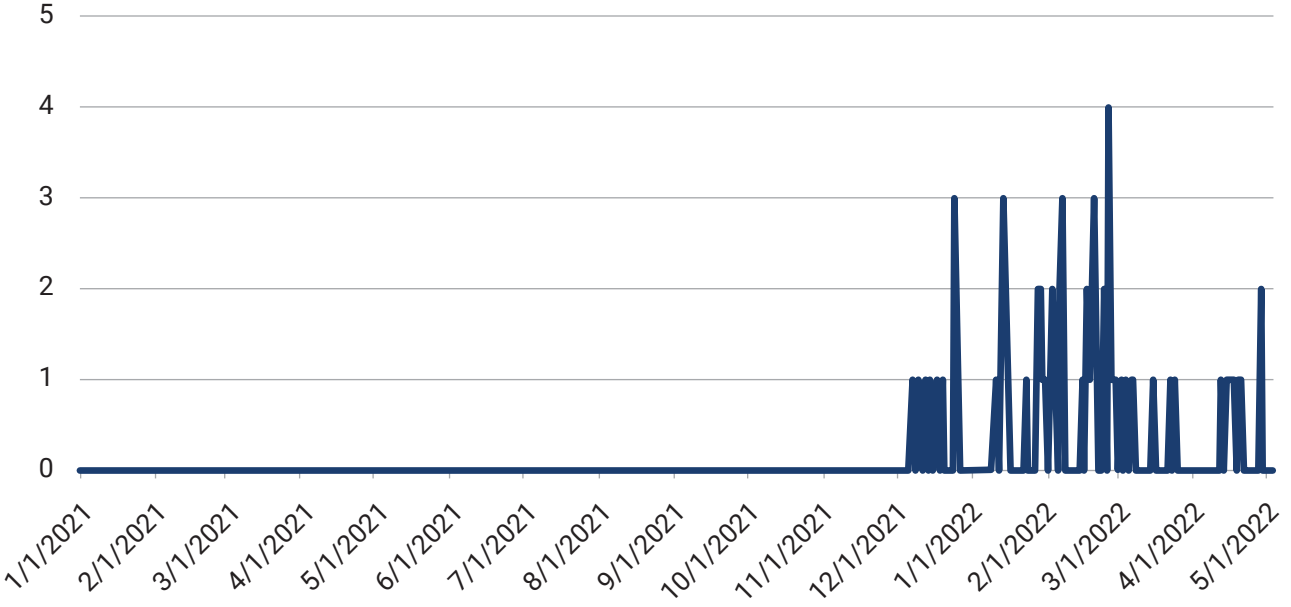
Number of *Nikkei Shimbun* articles containing the term "disinformation" (January 2000 to June 2022)



Source: Author calculations based on the Nikkei Shimbun's Nikkei Telecon 21 database.

FIGURE 3

Number of newspaper articles containing the term "NATO kakudai (NATO expansion)" (January 1, 2021 to May 3, 2022)



Source: Author calculations based on Asahi, Mainichi, Nikkei, and Yomiuri Shimbun databases. Asahi Shimbun database covers the Asahi Shimbun, AERA, and Weekly Asahi. Mainichi Shimbun database covers Mainichi Shimbun and Weekly Economist. Nikkei Shimbun database covers Nihon Keizai Shimbun, Nikkei Sangyo Shimbun, Nikkei MJ, and Nikkei Veritas. Yomiuri Shimbun databases covers Yomiuri Shimbun only.

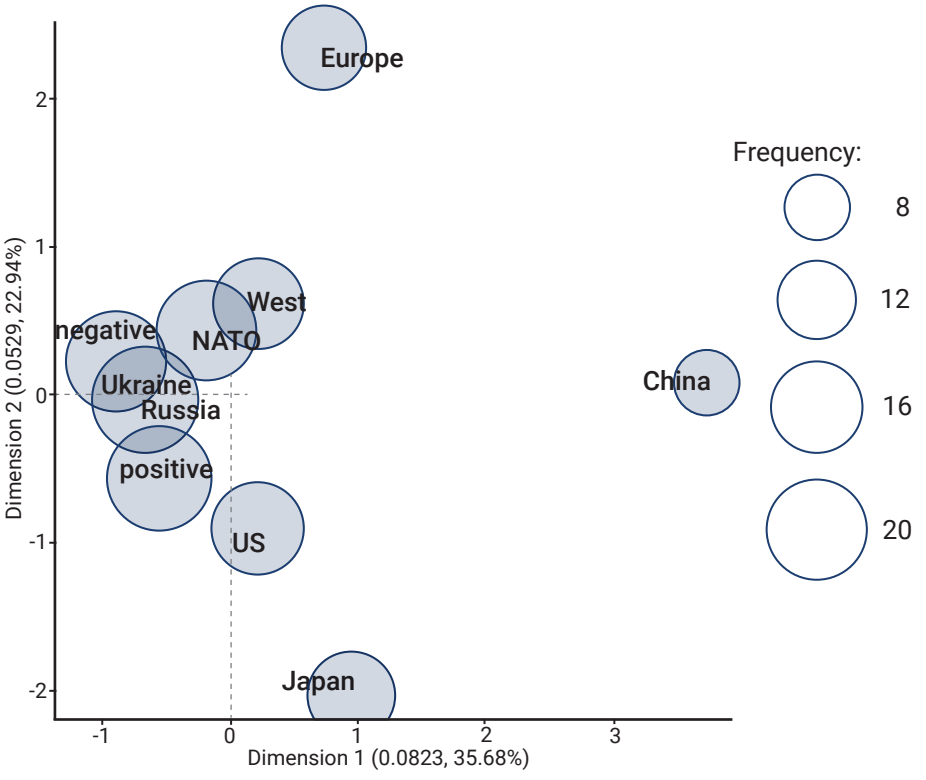
by Russia to justify its aggression). 71 articles with this keyword were found (figure 3), all of which appeared after Russia deployed troops surrounding Ukraine and began using NATO expansion as the cause.

Among them, sixteen articles contained whataboutism. Together with five other articles from outside these databases, this study analyzed which actors the writers found problematic and which actors they found justifiable. After categorizing the adjectives used in the articles into positive and negative adjectives, this study analyzed which type of adjectives were used in describing each actor, using KH Coder software. The result of the correspondence analysis is shown in figure 4. The terms that are used throughout these articles appear near the coordinate axis (0, 0), and the terms that tend to appear together and given interconnections are located close to one another. Since "NATO expansion" was used as a keyword in selecting the articles, many of the articles discuss the role of NATO and the West in addition to discussing negative and positive aspects of Russia and Ukraine. Further, the association of negative terms is somewhat stronger than that of positive terms with NATO and the West, which shows that many of these articles critically analyze NATO and the West and especially their expansion. Together with the fact that there was no article on the topic published until December 2021 (figure 3), this is a phenomenon not seen before Russia resorted to information warfare, which shows that the writers take the information spread by Russia seriously.

What this reveals is that references to China, Europe, and Japan are not very common. Two points come from this analysis. First, the writers do not seem to view China as an actor in the Russia-Ukraine war, which shows a limited awareness of the role of pro-Beijing trolls as

FIGURE 4

Correspondence analysis of articles that contain whataboutism



Source: Author calculations of articles collected from Asahi, Mainichi, Nikkei, and Yomiuri Shimbun databases using KH Coder.

spreaders of Russian disinformation. Second, the writers also do not seem to view Japan as an actor either, even though the Japanese government has imposed economic sanctions against Russia and has accepted displaced people from Ukraine. The finding indicates a weak sense of ownership of these decisions among the writers themselves, which may be why they do not find the necessity to make moral judgments for the lives, dignity, and state sovereignty of Ukraine.

The articles do criticize Russia's military aggression, stating that it cannot be justified and should end. However, as a way to end the war, they tend to call on Ukraine and the West to compromise. This stance not only shows little imagination as to what will happen to the people of Ukraine if they give up their territory, but also seems to indicate a resignation that Japan does not have leverage over Russia.

COUNTERMEASURES AGAINST DISINFORMATION IN JAPAN

This case of Russian disinformation reveals that countermeasures in Japan cannot focus only on tackling the origins of disinformation per se; they also need to prevent other domestic conspiracy theorists, trolls, and commentators of conscience from being unintentionally influenced by disinformation.

Before making recommendations, it is helpful to take stock of the current countermeasures. At the governmental level, there is no anti-fake news law in Japan. Such laws have been enacted around the world in recent years (largely in response to disinformation on COVID-19), but the Japanese government has not done so in order to guarantee freedom of expression.

The task of fact-checking has been left to private initiatives, and the growing awareness of disinformation since 2016 has led to an increase in the number of media and organizations conducting fact-checking in Japan. Today, major national newspapers such as *Nikkei*, *Asahi*, *Mainichi*, and *Sankei* have their own fact-checking functions, as do national broadcasters such as NHK and Nippon TV, regional newspapers such as *Ryukyu Shimpo* and *Okinawa Times*, regional TV stations such as Chukyo TV, and online media such as Buzz Feed Japan.

When Ukraine was invaded, the FactCheck Initiative Japan (FIJ), a networking organization of fact-checkers, created a special website to collect fact-checking results of disinformation and misinformation related to Russia's invasion of Ukraine.[8] The FIJ trains the next generation of fact-checkers and uses artificial intelligence to identify questionable discourse.[9] The Ministry of Internal Affairs and Communications has also been strengthening its cooperation with fact-checking organizations.

However, the overall volume of human resources in charge of fact-checking is far from enough. Each media outlet manually conducts fact-checking in the absence of excess human resources, which therefore limits the amount of questionable discourse they can check. There is also little information available on the number of instances of disinformation removed from online.[10]

At the governmental level, it was only recently that the analysis of disinformation began to expand. Given that disinformation is now a part of military strategy, on April 1, 2022, the Ministry of Defense created the position of Global Strategic Intelligence Officer, whose main mission is to analyze disinformation. The ministry also expanded the country's cyber forces.[11] In addition, it now disseminates information in not only Japanese but also in English, Chinese, and Korean for the purpose of responding to information warfare.[12] The human resources for these tasks remain far from enough, however.

When articles using whataboutism appeared after the Russia-Ukraine war began, international relations scholars with tens of thousands of social media followers tweeted and pointed out the problem with whataboutism. This helped to mainstream, and raise awareness of, the issue among the media, but it has not fundamentally addressed it.

POLICY RECOMMENDATIONS

Despite the above countermeasures, the Russian propaganda campaign continues to spread disinformation. What more should Japan do to limit it?

As hybrid warfare becomes mainstream and defense in the cognitive domain becomes increasingly important, the Japanese government should expand the resources devoted to disinformation analysis. And this effort should be conducted in collaboration with other democracies, so that countries can share experiences and information. For example, frameworks such as the Quadrilateral Security Dialogue should include countering disinformation as one of its pillars.

Tackling disinformation effectively requires remaining neutral and objective, so that counternarratives do not get politicized and dragged into the discursive war. In that sense, the private sector's role is vital in restraining disinformation. The establishment of the nongovernmental Japan Factcheck Center in October 2022, as a complement to the existing FactCheck Initiative Japan, is thus a welcome move.[13]

The media and academia also have vital roles. Trust in Japan's traditional media remains high, and their digital versions are read extensively online. Given the impact the media, and especially digital media, could make, they should publish more fact-check results as high-value news. The Huffington Post and BuzzFeed Japan have been setting a precedent in this practice, and their articles on fact-check results are widely accessed and read.

Writing the results of fact-checks in a simple black-and-white way, however, could potentially demonize conspiracy theorists and further polarize society. To avoid this, media outlets need to reach out to people across the political spectrum. Trying to understand what motivates people involved in conspiracy theories is important.

Explaining disinformation in a simple, easy-to-understand way is also necessary, given that people have various educational backgrounds. In that sense, the *Asahi Shimbun*'s recent approach was admirable — which was to answer questions that could potentially arise when people are exposed to Russian disinformation, using simple language that is not usually found in news articles. The answers used various examples from daily life and other international issues to make the explanations easy to understand, even for youth.[14]

Universities are the best places to train not only the next-generation researchers on disinformation, but also fact-checkers. Academic schools, however, tend to be slow in incorporating methods and arguments relevant to today's politics and international relations. Courses on contemporary issues should be offered, covering such topics as cybersecurity, disinformation, and artificial intelligence. Also, methodology classes should incorporate the scope of data science and cover the topics of scraping, programming, and content analysis.

Last but not least, universities should facilitate the sharing of scraped data and analysis software. Analysis software tends to be too costly for students to purchase, but if they were to be given free access, graduate students could write dissertations on the disinformation issue and generate substantial progress in the field. It would be a win-win for universities seeking to have a greater reputation both inside and outside the country.

REFERENCES

1 Morihiro Ogasawara, "Nihon no yukensha ha ikani nyusu wo feiku to ninshiki shitaka" [How Japanese voters recognized news as fake], in *Feiku nyusu ni shinkan suru minshushugi [Democracy shakes with fake news]*, ed. Seiko Kiyohara (Okayama: Daigaku Kyoiku Shuppan, 2019), 146.

2 Atsuo Fujimura, "Gijoho niyoru johososa to fakutotyekku" [Manipulation with Disinformation and Factcheck], in *Hakku sareru minshushugi: Dejitaru shakai no senkyo kansho risuku [Hacked Democracy: Risks of Election Interference in the Digital Society]*, Morohiro Tsuchiya and Takahisa Kawaguchi (Tokyo: Chikura Shobo, 2022), 127-129.

3 Puratto fomu sabisu ni kansuru kenkyukai [Study Group on Platform Services], "Puratto fomu sabisu ni kansuru kenkyukai" [Study group on platform services final report], Ministry of Internal Affairs and Communications, February 2020, https://www.soumu.go.jp/main_content/000668595.pdf.

4 Kazuki Ichida, *Feiku nyusu: Atarashii senryakuteki senso heiki [Fake news: The new strategic warfare weapon]* (Tokyo: KADOKAWA, 2018); Kazuya Matsumoto, *Dipuefiku to tatakau: 'Suro janarizumu' no jidai [Fighting deep fake: The age of 'slow journalism']* (Tokyo: Asahi Shimbun Publishing, 2019); Morihiro Ogasawara, "Nihon no yukensha ha ikani nyusu wo feiku to ninshiki shitaka: 2017 nen shuinsen niokeru 'feiku nyusu' no ninchi" [How Japanese voters recognized news as fake: Perception of 'fake news' in 2017 House of Representatives election], in *Feiku nyusu ni shinkan suru minshushugi: Nichibeikan no kokusai hikaku kenkyu [Democracy shakes with fake news: International comparative studies of Japan, US, and South Korea]*, Seiko Kiyohara (Okayama: Daigaku Kyoiku Shuppan, 2019), 122-150; Shojiro Okuyama, "Whebu medhia uneisha no shiten kara kosatsu suru nihon niokeru feiku nyusu kakusan no shikumi" [A web media operator's perspective on the mechanism of the spread of fake news in Japan], in *Feiku nyusu ni shinkan suru minshushugi: Nichibeikan no kokusai hikaku kenkyu [Democracy Shakes with Fake News: International Comparative Studies of Japan, US, and South Korea]*, Seiko Kiyohara (Okayama: Daigaku Kyoiku Shuppan, 2019), 151-172; Yoichiro Tateiwa, *Fakuto chekku saizensen: Feiku nyusu ni honro sarenai shakai wo mezashite [The forefront of fact check: Aiming at a society which does not rack with fake news]* (Tokyo: Akebi shobo, 2019); Yoichiro Tateiwa and Hitofumi Yanai, *Fakuto chekku toha nanika [What is fact check]* (Tokyo: Iwanami shoten, 2018); Motohiro Tsuchiya and Takahisa Kawaguchi, *Hakku sareru minshushugi: Dejitaru shakai no senkyo kansho risuku [Hacked democracy: Risks of election interference in the digital society]* (Tokyo: Chikura Shobo, 2022).

5 "SNS de 'higai ha ukuraina no jisakujien' kakusan, inboron ni tsugitsugi keito no wana... ukabu kyotsuten" ['Damages in Ukraine are self-made' Spread on SNS, and people are falling for conspiracy theories one after another... some commonalities], *Yomiuri Shimbun*, April 14, 2022, https://www.yomiuri.co.jp/national/20220414-OYT1T50064/.

6 Gakushi Fujiwara, "Nihon demo hirogaru 'Q anon' shinjiru hito mo shinjinai hito nimo todoketai jijitsu" ['Q Anon' spreading in Japan: Facts for believers and non-believers alike], *Asahi Shimbun*, April 12, 2022, https://digital.asahi.com/articles/ASQ4B7GWWQ49UHBI01N.html?iref=pc_ss_date_article; "'Damages in Ukraine are self-made' spread on SNS," *Yomiuri Shimbun*.

7 Kenji Ando, "Kawase naomi kantoku no todai nyugakushiki deno shukuji, kokusai seiji gakusha kara hihan aitsugu, 'shinryaku senso wo aku to ienai daigaku nante hitsuyo nai'" [Naomi Kawase's congratulatory address at the University of Tokyo entrance ceremony draws criticism from international relations scholars, saying 'we don't need a university that can't call wars of aggression evil,'" *Huffpost*, April 13, 2022, https://www.huffingtonpost.jp/entry/shukuji_jp_625625c7e4b0be72bfefec0d.

8 "Ukuraina kanren no fakuto chekku" [Fact Check Related to Ukraine], FactCeck Navi, FactCheck Initiative Japan, https://navi.fij.info/factcheck_navi_tag/ukraine/.

9 Atsuo Fujimura, "Manipulation with Disinformation and Factcheck," 137-139.

10 "Nise nyusu taisaku he choshu: Somusho, guguru ya meta taisho" [Hearing to combat fake news: Ministry of Internal Affairs and Communications targets Google and Meta], *Nikkei Shimbun*, March 29, 2022, https://www.nikkei.com/article/DGKKZO59479040Y2A320C2EP0000/.

11 "Roshia shinko, SNS mo senjo haiburiddo sen" [Russian invasion, SNS are also battlefields: Hybrid warfare], *Asahi Shimbun*, April 3, 2022, https://digital.asahi.com/articles/DA3S15255287.html?iref=pc_ss_date_article.

12 "Boeisho ga 'johosen' kyoka, chugokugo ya kankokugo demo SNS toko... nichibei kyodo kunren wo apiru" [The Ministry of Defense is strengthening 'information warfare,' posting on SNS in Chinese and Korean as well... appealing the Japan-U.S. joint drill], *Yomiuri Shimbun*, April 30, 2022, https://www.yomiuri.co.jp/politics/20220430-OYT1T50241/.

13 Japan Factcheck Center, "JFC nitsuite" [About JFC]. https://factcheckcenter.jp/n/n50986dc9216c.

14 "'Roshia ha aku' iikireru riyu ha? Ukuraina shinko, judai no gimon" [What makes you say 'Russia is evil'?: The invasion of Ukraine, teenagers' questions], *Asahi Shimbun*, March 30, 2022, https://digital.asahi.com/articles/ASQ3X7DHNQ3XULEI00K.html.

DISINFORMATION AND DEMOCRACY IN MALAYSIA

NUURRIANTI JALLI

THE CURRENT STATE OF MIS/DISINFORMATION IN MALAYSIA

The increased penetration of Internet connection in Malaysia and high mobile device affordances in Malaysia over the last two decades resulted in significant changes in the media ecosystem and information consumption patterns in Malaysia[1]. Like in many parts of the world, one of the side effects of increased liberation of information production in Malaysia is the flooding of mis/disinformation, particularly in cyberspace. This paper will focus specifically on political mis/disinformation, government responses to this pressing issue, and some suggestions for Malaysian policymakers to improve current mitigation efforts.

MISINFORMATION	DISINFORMATION
False or misleading information *unintentionally* shared with recipients. Often driven by socio-psychological factors[2] such as personal bias, lack of understanding on information-context, as well as lack ability to fact-check information found (low media and information literacy).	Fabricated or *deliberately* manipulated content to deceive recipients. Typically motivated by three factors, to make money, to influence (either foreign or domestic), or to cause harm[3].

Cybertroopers and political information warfare

The advancement of information technology has given birth to novel disinformation techniques such as the use of deepfakes, the bombardment of false information (often called a firehose of falsehood), and the deployment of cybertroopers (paid political cyberarmies) to shape public opinion. In Malaysia, as internet access and service have continued to improve, cybertroopers have found the use of strategic information warfare, particularly on social media platforms, beneficial in mounting disinformation campaigns for political ends.

Because of the low level of media and information literacy among Malaysian society, online disinformation campaigns have become prime political warfare tools in the country. Cybertroopers actively employ computational disinformation campaigns (through information manipulations and the distortion of truth) to continuously influence political discourse. While using mis/disinformation for political ends is definitely not a recent phenomenon in Malaysia — the government has long used traditional media outlets such as TV, radio, and the printing press as propaganda mouthpieces — the availability of social media, high internet access, and increased digital device affordances contribute to a broader employment of novel disinformation techniques.[4]

The deployment of cybertroopers to assist with disinformation campaigns, especially during the election period in Malaysia, is now a contemporary fixture in the country's politics. First associated with the political coalition Barisan Nasional,

the term "cybertrooper" is used to describe political cyberarmies in Malaysia. Barisan Nasional is led by the United Malays National Organization (UMNO) and has been the most dominant coalition in Malaysian history. It has been in power since the independence of Malaya (peninsular Malaysia) in 1957, except from 2018 to 2019, when the coalition lost its first general election to the opposition coalition, Pakatan Harapan.

During interviews with Barisan Nasional cybertroopers in 2018, they stated that the goal of election disinformation campaigns, particularly on Facebook and WhatsApp, was to craft positive images of Barisan Nasional's politicians, particularly Najib Razak as he was muddled in a massive corruption scandal called 1MDB.[5] A former Barisan Nasional's cybertrooper noted, "We [the coalition] have to create a [negative] perception [of Pakatan Harapan], so the public will hate Pakatan." Aimed at influencing individuals with low media and information literacy, the campaigns were designed to demonize political opponents in the general election by creating inflammatory content centered on race, religion, and the royals/monarchy.

In Malaysia's eastern states Sabah and Sarawak, the cybertroopers crafted targeted disinformation campaigns using indigenous languages, as the demography of the population in these states is much more diverse than in western Malaysia. In Sabah and Sarawak, Christian and indigenous groups make up the majority, not Muslims and Malays. According to a few cybertroopers interviewed, drafting content in local languages and dialects was highly important for reaching the people of these two states because English and Malay are not their mother tongues. The cybertroopers believed that content created in the people's native languages would be more credible and bridge the communication gap between the messenger and receiver of the information. One cybertrooper said, "It is important for us to be aware of the dominant language spoken in the targeted population. I can't create content in Bahasa Semenanjung (Eastern Malaysians tend to call formal Bahasa Malaysia as Bahasa Semenanjung, or loosely translated as the Peninsular Malay language) when people speak Iban [one of the Dayak ethnic group's languages] in the longhouses in Kapit [a town in Sarawak]. There would be a gap, as they don't feel the sense of closeness to the messenger."

Communication strategists and politicians have long understood the power of indigenous languages to mobilize the support of local people.[6] Having realized that political success largely depends on rural society, politicians, especially in Sabah and Sarawak, actively used indigenous languages in their campaigns, advertisements, and other mobilization activities. To win an election in these two states, using indigenous languages to propagate pro-party narratives has proven to be crucial, as content in English and Malay could be viewed as coming from "foreign actors" (those in western Malaysia); people in the eastern states, particularly Sarawak, reject the interference of "Malay politics," particularly of the UMNO. Therefore, for local cybertroopers — especially those associated with Sarawak Barisan Nasional, now Gabungan Parti Sarawak — both curating persuasive disinformation messages in local languages and dialects and determining the right platform to share these messages are crucial. For Sarawak, cybertroopers have mainly used Facebook and WhatsApp.

Online disinformation campaigns launched in local indigenous languages and dialects are hard to trace, especially with existing analytic tools offered by tech companies. Disinformation propagated by cybertroopers likely remains on social media unless other users report the content to local authorities or the platform moderators. With the popularity of encrypted free-text messaging apps like WhatsApp in Malaysia, tracing disinformation campaigns becomes almost impossible, enabling mis/disinformation to continue influencing public opinion.[7]

Automated bots and semi-bots and the spread of mis/disinformation

In addition to curating contentious, false, and misleading content for social media during the 2018 general election, cybertroopers used automated bots and semi-bots, particularly on Twitter, to silence critics and spread pro-Barisan Nasional messages and artificial narratives. For example, #PulangMengundi (go home to

vote) was hijacked by thousands of bots and semi-bots launched by Barisan Nasional's cybertroopers. The #PulangMengundi hashtag was meant to connect people who needed help traveling to their hometowns to vote with people who were willing to help them, either through monetary donations or carpooling.[8] The #PulangMengundi hashtag came about as a criticism of, and response to, the government's announcement (under then Prime Minister Najib Razak) to hold the election on Wednesday, May 9, 2018. Traditionally, polling is held on weekends in Malaysia to allow people to travel to their hometowns where they are registered to vote.[9] Critics saw the odd date as a methodological approach by the incumbent Barisan Nasional government to lower voter turnout and thereby help Razak remain the prime minister. As the hashtag gained traction, many pro-Barisan Nasional/pro-government Twitter accounts used the same hashtag to drown out the call for voting help and the criticism of the government.

These anonymous accounts also added, alongside #PulangMengundi, hashtags like #SayNOtoPH (say no to Pakatan Harapan, which was the leading opposition during the 14th general election) and #RespectMYPM (respect my prime minister). Thousands of Twitter accounts shared thousands of such tweets, which were automatically shared with all of #PulangMengundi's hashtag followers to drown legitimate calls for help and sway voters to support the incumbent party.

Aforementioned events illustrate how the fluidity of internet content opens door for mis/disinformation to cross platforms, damaging people's ability to make informed decisions, including choosing leaders based on factual information and authentic political debates. Until today, cyber disinformation operations remain prevalent in Malaysia despite attempts to mitigate through the enactment of "fake news" laws and policies as well as concerted efforts by nongovernmental actors. As Malaysia heading to its next general election, coordinated disinformation campaigns are expected to continuously used to gain and maintain unchecked power. If not properly addressed, this could contribute to the corroding democracy in the country.

Screenshot of a tweet posted by a suspected bot on April 17, 2018, less than a month before Malaysia's 14th general election in 2018. While many of these tweets are no longer on Twitter post Malaysia's 14th general election, the strategic use of bots to drown calls for help was a concern for many Twitter users during the 2018 election. Image retrieved from Twitter user @iamnormgoh.

GOVERNMENT RESPONSES

According to the prevailing criticism, government attempts to address severe information pollution in Malaysia continue to be loosely defined and biased. In particular, civil society[10] critics view the government's recent bills and laws aimed at curbing orchestrated disinformation campaigns as weapons to strengthen the state's political holds[11].

Policies and practices to mitigate information disorders in Malaysia

Anti-Fake News Act 2018

While various Malaysian laws impose penalties for sharing false information — such as the Malaysian Penal Code, Printing Presses and Publications Act 1984, and Communications and Multimedia Act 1998 — the Barisan Nasional-led administration of Razak introduced the Anti-Fake News Act 2018 as another instrument to address fake news and rumor-mongering. Some in civil society saw[12] the move as the state's attempt to further restrict freedom of expression in the guise of "countering mis/disinformation ."[13] They claimed that with the loose definition of what constitutes fake news, the act could be used strategically as a political weapon. In response, the government argued that the existing laws were insufficient to address complex challenges that arise from the large amount of false information in Malaysian cyberspace due to technological advancements. Thus, despite the backlashes, the law went into force. The Anti-Fake News Act 2018 could be used to charge any individuals, regardless of their citizenship and their locality, for spreading "fake news" related to Malaysia or affects a Malaysian citizen. The impact of this provision could influence Malaysia's international relations, particularly with other democratic countries with high freedom of expression. However, after Razak lost in the 2018 general election, the law was repealed in October 2019 by then Prime Minister Mahathir Mohamad, the leader of Pakatan Harapan.

Emergency (Essential Powers) (No. 2) Ordinance 2021

On March 12, 2021, following the Emergency Proclamation invoked in January 2021 by then Prime Minister Muhyiddin Yassin of Perikatan Nasional, the government enacted the Emergency (Essential Powers) (No. 2) Ordinance 2021 without parliamentary approval. (The legislative body had been suspended during the state of emergency, leaving Malaysia without democratic oversight for several months.) The ordinance — intended to combat fake news related to COVID-19 and the Emergency Proclamation — was heavily criticized, viewed as an attempt by Yassin to muzzle criticism of his administration's handling of the COVID-19 pandemic.

Under the ordinance, individuals who spread fake news in writing, videos, audio recordings, or in any other forms that may convey "words or ideas" if found guilty faced a jail term of up to three years or a fine up to 100,000 Malaysian ringgit (20160 US dollars) or both. Any parties who provided "financial assistance" intended for "committing or facilitating" such fake news were also liable for a jail term of up to six years or a fine of up to 500,000 Malaysian ringgit (108, 003 US dollars) or both. As the definition of "fake news" was broadly defined in the ordinance, it gave the government total power to decide what was true or false and also the authority to remove any publication determined to contain inaccurate information. Additionally, the ordinance gave the military police powers, allowed the forced confiscation of property with no ability to challenge the compensation offered, and provided the government and military near-total impunity for acts taken under the ordinance. The ordinance also indefinitely postponed the holding of any elections and the sitting of the country's Parliament and state assemblies.

When the state of emergency in Malaysia ended in August 2021, the public was unsure if all ordinances related to the Emergency Proclamation would be annulled by Parliament. It was not until October 2021 that Minister in the Prime Minister's Department (Parliament and Law) Datuk Seri Wan Junaidi stated that all emergency-related ordinances — except those provisions that were explicitly set to end with the expiration of the proclamation — would still be enforceable until revoked or until the end of a six-month grace period following the proclamation's conclusion (in other words, February 2022).[14] The decision was not well received by the public particularly in the state of Sarawak, where the move was seen to be politically motivated as it put the state election on hold[15].

Campaigns by the Malaysian Communication and Multimedia Commission

In 2017, the Ministry of Communications and Multimedia, through the Malaysian Communications and Multimedia Commission,

established Sebenarnya.my as a one-stop website for Malaysians to verify the authenticity of viral information they found online. However, since Sebenarnya.my is a government's brain-child, critics are skeptical that the website provides the truth to the public, particularly on content related to the government in power. Additionally, Sebenarnya.my has been criticized for not making regular updates on its website and social media regarding recent false viral content. Therefore, despite also having Facebook and Telegram accounts and an app, it has not gained traction in Malaysian society. Sebenarnya.my's Facebook page only has 18,000 followers and the posts are infrequent.

Tidak Pasti Jangan Kongsi (if not sure, don't share) is Sebenarnya.my's slogan and is used by the Malaysian Communications and Multimedia Commission for a nationwide campaign on fighting mis/disinformation online. While this campaign is well-known in Malaysia, as it is often broadcasted through national television channels, radio, and social media, it mostly focuses on reminding Malaysians not to share unverified content on the internet. The campaign does not put enough stress on teaching people the skills to spot mis/disinformation.

RECOMMENDATIONS

The next section of this paper offers recommendations for the Malaysian government and nongovernmental actors to mitigate mis/disinformation, particularly focusing on these multiprong approaches:

- Place more emphasis on media and information literacy education, not legislation
- Provide communities media and information literacy training
- Establish cohesive, independent monitoring and fact-checking agencies
- Invest in research and projects focused on counter- mis/disinformation strategies
- Increase media freedom and allow for transparent journalism
- Increase the quality of journalism

Place more emphasis on media and information literacy education, not legislation

Despite existing laws covering false information in Malaysia, the government enacted two more laws specific to fake news. Both laws were criticized for the same reasons: the redundancy of purpose (due to other existing media related laws in Malaysia) and their broad and vague definition of what constitutes false information. Unless if Malaysian government and lawmakers can come up with clear and specific definitions of what constitutes 'false information', enacting new laws should be carefully thought; as vague definition can open doors for inconsistent enforcement by authorities and parties with vested interests.

While working on construction of better legal framework, government efforts should also be focused on equipping Malaysians with the right media and information literacy skills to help them spot mis/disinformation. In Malaysia, to date, a multiplatform media and information literacy curriculum has yet to be developed as a required subject in schools and higher-learning institutions. In Finland, incorporating media and information literacy curriculum in educational institutions has yielded results, making it one of Europe's most resistant nations to fake news.[16] For Malaysia, any curriculum for media and information literacy should first be reviewed by independent, external reviewers to ensure that the learning materials are justified and to avoid weaponizing media literacy programs for government propaganda, as observed in Indonesia.[17]

Provide communities media and information literacy training

Media and information literacy training should also be provided to the community, and the modules should be developed in the dominant languages spoken within the community. Then, since ethnic, religious, and district leaders have played a significant role over the years in shaping public opinion on socioeconomic issues, some of these leaders should be a part of the media and information literacy initiatives

to help convince people to participate in the training. Media and information literacy ambassador programs could be created nationwide to elect ambassadors to continually teach their respective communities new media and information literacy skills, including fact-checking. The failure to provide enough education and training has made Malaysians susceptible to mis/disinformation spread by local or foreign actors for political or financial ends. In Malaysia, between 2019 and 2021, 16.1 billion Malaysian ringgit (3.46 billion US dollars) was lost to scammers, with many of the 51,631 cases reported involving cyber-operationalists from foreign countries.[18] By continually providing high-quality media and information literacy training, the public will eventually be better equipped to evaluate content they read and protect themselves online. Additionally, through awareness campaigns, Malaysians should be taught to be more skeptical of online information and to take extra initiatives to fact-check content containing provocative information. As propaganda and politically driven disinformation is rampant online, Malaysians should also be encouraged to follow diverse people and perspectives to prevent the formation of an information bubble, which could create a narrow view on various issues. In some instances, information bubbles have created radicalized followers and supporters of certain ideologies. This extremism could potentially jeopardize national security.

Establish cohesive, independent monitoring and fact-checking agencies

Independent monitoring and fact-checking agencies should be set up (free from state funding and influence) to ensure impartiality in reporting. There is no local independent fact-checking agency actively informing Malaysians about falsehoods viral on social media. In the Philippines, VERA Files, a nonprofit independent media organization, actively uses social media to educate the public daily on fake news circulating in the country's cyberspace. Malaysia needs an agency like VERA Files to help with the counter-disinformation initiative. The agency's content moderators should be able to speak and read indigenous languages at sufficient levels to ensure that vulnerable indigenous communities in Malaysia are also protected from mis/disinformation.

Invest in research and projects focused on counter-disinformation strategies

More funds from government agencies and independent parties should be allocated to research and projects related to counter-disinformation strategies. Government-funded projects should focus on in-depth studies of counter-disinformation initiatives, particularly related to public health threats (such as COVID-19) as the government's current methods to handle disinformation in this area could be further improved. Data from research could assist the Malaysian government in developing a better national strategic response to mis/disinformation and could eventually help mitigate distrust toward the government. Independent parties, such as local think tanks and other nongovernmental agencies, should also increase their financial support of research related to mis/disinformation to ensure that comprehensive data can be obtained on Malaysia. Data reported by independent agencies could be compared with the government's findings to help decrease the chances of data being weaponized for political gain. Local entities, including government agencies, autonomous bodies, and media houses, should also establish or increase collaboration with tech powerhouses such as Meta, Twitter, Google, and ByteDance to better understand how their platforms could help with counter-disinformation initiatives and to protect the freedom of speech of their users.

Increase media freedom and allow for transparent journalism

Distrust toward traditional mainstream media (TV, radio, newspapers) should be looked at seriously by the government. Historically, Malaysian media outlets have served as government mouthpieces, resulting in constant distrust of the local press. Ultimately, this distrust led Malaysians to turn to online sources, which increased the likeliness of exposure to mis/disinformative content. To address this issue, the government should look at ways

to alleviate public distrust of mainstream media. It could (1) reform media laws — particularly the Communications and Multimedia Act 1998, which gives the Minister of Communication arbitrary power to grant and revoke licenses and penalize media agencies; (2) uphold the concept of a free press and freedom of expression as guaranteed in the Malaysian constitution; (3) review media ownership by government-affiliated conglomerates; (4) reform current traditional mainstream media practices by permitting critical sociopolitical reporting to be broadcasted and shared on these platforms.

For their part, media practitioners and the public should make stronger calls for a free press and government transparency in order to help push for reforms in the media landscape. Taking immediate action, via global platforms, to report violations of press freedom would help to highlight cases of censorship, the revocation of operation permits, politically motivated raids, and the unlawful detainment of journalists. Currently, as a result of powerful political influence, the practice of self-censorship among journalists is common in Malaysia. If the practice continues, it will further undermine democracy in the country.[19]

Increase the quality of journalism

The Malaysian news industry should focus on increasing the quality of journalism to attract audiences and gain their trust. In particular, news agencies that publish in local languages and dialects should hire more multilingual, well-trained journalists to avoid substandard reporting. In addition to increasing the quality of news reports, news agencies and journalists should also consider creative ways to deliver the content to the public. Creating news bites using social media templates is one of the most effective approaches, considering that Malaysians access social media much more often than traditional media.[20] Short documentaries and transmedia storytelling also could potentially attract more people to subscribe to professional journalism. Finally, news agencies should establish a solid fact-checking department to help verify information before news reports are published.

REFERENCES

1 Bahiyah Omar, Nurzali Ismail, and Ng See Kee. "Understanding online consumption of public affairs news in Malaysia: a strategic approach." *Journal of Asian Pacific Communication*, 28(1), (2018): 172-194. https://www.jbe-platform.com/content/journals/10.1075/japc.00009.oma.

2 Claire Wardle "Understanding Information Disorder," *First Draft,* September 22, 2020, https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

3 Claire Wardle, "Understanding Information Disorder."

4 Zafira Syamim Anwar and Nuurrianti Jalli, "Wahyu dah Kurang: Journalism Practice Among Journalists in Malaysian Mainstream Media Agencies during Pakatan Harapan Tenure," *Journal of Media and Information Warfare* 13, no. 2 (December 2020): 17-30, https://www.researchgate.net/publication/348078214_Wahyu_dah_kurang_Journalism_Practice_Among_Journalists_in_Malaysian_Mainstream_Media_Agencies_during_Pakatan_Harapan_Tenure.

5 Nuurrianti Jalli and Ika Karlina Idris, "Fake News and Elections in Two Southeast Asian Nations: A Comparative Study of Malaysia General Election 2018 and Indonesia Presidential Election 2019," *Advances in Social Science, Education and Humanities Research* 367 (2019): 138-148, https://www.atlantis-press.com/proceedings/icdesa-19/125923267.

6 Ayo Ojebode and Wole Oladapo, "The power of truth-drive propaganda: A rhetorical criticism of governor Ajimobi's political slogan: 'ki oyo le da'a ajumose gbogbo wa ni'," *Research in African Languages & Linguistics* 13 (April 2014): 39-58, https://www.researchgate.net/publication/280075564_THE_POWER_OF_TRUTH-DRIVEN_PROPAGANDA_A_RHETORICAL_CRITICISM_OF_GOVERNOR_AJIMOBI'S_POLITICAL_SLOGAN_'KI_OYO_LE_DA'A_AJUMOSE_GBOGBO_WA_NI'.

7 Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," (Oxford: Project on Computational Propaganda, 2018), https://holbrook.no/share/papers/computational_social_media_fake.pdf.

8 Pauline Pooi Yin Leong, "New Media and Political Change." In Malaysian Politics in the New Media Age, pp. 147-160. Springer, Singapore, 2019. https://link.springer.com/book/10.1007/978-981-13-8783-8.

9 Abby Selff, "This Country's Election Shows The Complicated Role Twitter Plays In Democracy," Huffpost, May 5, 2018, https://www.huffpost.com/entry/twitter-malaysia-elections_n_5aeafdd5e4b00f70f0efe0bf.

10 SUHAKAM "Press Statement No. 13-2021_Government's Announcement on the Emergency (Essential Powers) (No. 2) Ordinance 2021 [PU (A) 110]", March 16, 2021, https://suhakam.org.my/2021/03/press-statement-no-13-2021_governments-announcement-on-the-emergency-essential-powers-no-2-ordinance-2021-pu-a-110/.

11 Article 19 "Malaysia: Repeal 'fake news' emergency ordinance," March 15, 2021, https://www.article19.org/resources/malaysia-fake-news-ordinance/.

12 Samantha Ho, "Malaysia Bill carries 'unduly broad definition for fake news' — Suaram," March 27, 2018. https://www.theedgemarkets.com/article/malaysia-bill-carries-unduly-broad-definition-fake-news-%E2%80%94-suaram.

13 Gulizar Haciyakupoglu, "Malaysia's Elections and the Anti-Fake News Act - How will the controversial new law affect the GE14 campaigns, and beyond?" April 26, 2018, https://thediplomat.com/2018/04/malaysias-elections-and-the-anti-fake-news-act/.

14 Kenneth Tee, "Law minister confirms Emergency ended in Aug, but says ordinances still apply until Feb 2022," *Malay Mail*, October 1, 2021,

https://www.malaymail.com/news/malaysia/2021/10/01/law-minister-confirms-emergency-ended-in-aug-but-says-ordinances-still-appl/2009806.

15 Dayak Daily, "Please wait, Sarawak govt will issue official response to lifting of Emergency Ordinance, DCM tells press," November 4, 2021, https://dayakdaily.com/please-wait-sarawak-govt-will-issue-official-response-to-lifting-of-emergency-ordinance-dcm-tells-press/.

16 Eliza Mackintosh and Edward Kiernan, "Finland is winning the war on fake news. What it's learned may be crucial to Western democracy," CNN, May 1, 2019, https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

17 Ika Karlina Idris, "Indonesia's misinformation program undermines more than it teaches," 360info, February 14, 2022, https://360info.org/indonesias-misinformation-program-undermines-more-than-it-teaches/.

18 Nuradzimmah Daim, "Online scammers rake in RM1.6 billion, over 51,000 reports lodged in 2 years," *New Straits Times*, March 14, 2022, https://www.nst.com.my/news/nation/2022/03/779915/online-scammers-rake-rm16-billion-over-51000-reports-lodged-2-years.

19 Zafira Syamim Anwar and Nuurrianti Jalli, "Wahyu dah kurang."

20 Kee, Ng See, and Bahiyah Omar. "Web interactivity and news credibility: Which is the stronger predictor to online news consumption in Malaysia?." SEARCH Journal of Media and Communication Research, Special Issue (2020): 89-106 https://www.researchgate.net/profile/See-Kee-Ng/publication/343721412_Web_interactivity_and_news_credibility_Which_is_the_stronger_predictor_to_online_news_consumption_in_Malaysia/links/5f3bd40b299bf13404cd75d3/Web-interactivity-and-news-credibility-Which-is-the-stronger-predictor-to-online-news-consumption-in-Malaysia.pdf.

DISINFORMATION IN TAIWAN

PUMA SHEN

DEFINING THE CHALLENGE

In Taiwan, the disinformation challenge is mounting, due to not only internal tension between political parties but also China's information operations. The lessons that can be drawn from the situation Taiwan faces are not limited to Taiwan: they are also applicable to other countries that have experienced a Chinese diaspora. The challenge is to differentiate between Chinese attacks and domestic division of opinion.

Taiwan has been ranked the number one country targeted by false information since 2013.[1] Because its official language is Mandarin, the country is particularly vulnerable to information and disinformation produced by China. The amount of disinformation produced by Taiwanese citizens pales in comparison to the volume coming from China.[2] Furthermore, Chinese operations include both the production and dissemination of disinformation. China can easily spread and amplify certain disinformation messages produced in Taiwan to increase their reach.

Three drivers, or flows, support the dissemination of disinformation:[3]

1. The information flow. This driver includes information directly produced and disseminated by China. The Communist Party's Central Propaganda Department, the Communist Youth League of China, the People's Liberation Army, Chinese netizens, and political content farms are all players involved in China's operations. Their efforts are often politically driven. In 2017 and 2018, most operations happened on Facebook, but since 2019, they have gradually moved to YouTube.[4] That year, Facebook started to remove fake accounts that post foreign content farm articles, and in response, China's operation actors started to turn these articles into text-to-speech YouTube videos and post the links on Facebook (YouTube links cannot be prohibited). For example, during the 2021 outbreak of COVID-19 cases in Taiwan, YouTube channels established by China that had mainly discussed conspiracy theories up until that point attracted 30 million view counts in three months, according to one analyst's calculations.[5]

2. The money flow. This driver includes information not directly produced by China. In this case, China only invests in the disinformation effort. Actors in Cambodia, Malaysia, and even Taiwan receive money from China, further contributing to the disinformation market. Their efforts are largely money-driven.[6] They receive interest through various means, including donations via live streams. Most of the operations use bot-like fake accounts that run only for certain periods of time and post Chinese content farm articles simultaneously.

3. The human flow. This driver often involves the Chinese United Front Work system — a global system that establishes relationships among like-minded individuals and organizations who are also capable of spreading disinformation. By "making friends" with like-minded, pro-China citizens around the world, including the diaspora, China can easily motivate these citizens to produce pro-China and/or anti-U.S. messages that align with the messages from the Central Propaganda Department. These actors are ideology-driven. They do not directly receive orders or interest like those in the above two categories, but they can still inject conspiracies into society. Businesspeople, professors, and retired officials are all examples

of possible players in this field. In addition to "weaponizing" social media, these actors can also be "weaponized," a tactic that authoritarian countries frequently employ to destabilize society.

All three drivers are not Taiwan-specific, but Taiwan faces more "human flow" than other nations due to its close ties with China. In addition, actors around the world may collaborate to initiate disinformation campaigns. For example, the abovementioned COVID-19 conspiracy theories targeting Taiwan were disseminated by fake accounts produced in Algeria, Cambodia, China, and Russia. Notably, the accounts used Mandarin, a language not understood by many in these countries' information space. Previously, the disinformation campaigns may have only included actors who speak Mandarin or write in Chinese. Now, due to advances in artificial intelligence technology, it is easy to generate content in a language the actors do not know, which poses a greater challenge in the digital environment.

GOVERNMENT AND CIVIL SOCIETY RESPONSES

The Taiwanese government has a team that deals with fake news, but the effectiveness of its efforts is constrained by the team's small scope. The Taiwanese government, due to its limited capacity, only focused on news that could be "debunked," which is why the government explicitly used the term "fake news" in its publicized policies. Although the government has adopted several strategies to combat fake news, civil society is still a key player in countering disinformation. This whole-society approach, however, has been facing huge challenges since the end of 2020, when there was a backlash against "debunking." On November 3, news reports revealed that the government was providing the debunked messages to online influencers, which created a conspiracy that the government was initiating its own "cognitive warfare."[7]

In 2018, the government launched a Disinformation Coordination Team (DCT) led by Lo Ping-Cheng, a minister without a portfolio. The team suggested four steps for stopping disinformation: identification, debunking, combatting, and punishment. For debunking, the DCT also suggested several principles such as "humor over the rumor" and the "222 principles" ("Each memeified debunking message shall contain no more than 20 characters in its title, no more than 200 characters in its content, and no more than 2 images appended").[8] The DCT collaborated with each government department to identify fake news (the news that could be debunked in their view) and to respond to it in several hours.

This process seemed to work well initially but has since encountered several obstacles. First, the debunking step only applies to fake news. Although conspiracy theories are also a major part of disinformation campaigns in Taiwan, it can be extremely difficult to debunk them due to their nature (for example, saying that the president is not healthy or the Democratic Progressive Party is too close to a certain entrepreneur). Conspiracies use layers of opinions to convince readers that "the world is not what they think" — and thus create distrust. Second, the punishment step has attracted criticism that it infringes on the freedom of speech. Third, although the department's adoption of the 222 principles makes the debunking process efficient, this swift response system has backfired at times. For instance, as noted above, the government used to provide the debunked messages to online influencers to "spread the word" quickly, and sometimes those influencers released them earlier than the government did, leading people to level the charges of favoritism and possible internal propaganda.[9]

Given the limitations in government initiatives, Taiwanese civil society continues to play a significant role in combatting disinformation. The efforts of civil society groups are relatively decentralized in comparison to those of the government. Several nongovernmental groups debunk messages daily or weekly (for example, the Taiwan FactCheck Center, MyGoPen, and Cofacts); some focus on investigating the cyber army, including bots, fake accounts, and trolls (for example, the Doublethink Lab and the Institute for National Defense and Security Research); and others focus on hosting workshops that inform citizens of the dangers of disinformation (for example, the Fakenews Cleaner and Chat for Taiwan). Although some of these groups have

working relationships, sometimes collaborate, and even have monthly meetings with each other, they do not seem to interfere with each other's tasks. Therefore, if a group receives public criticism, the criticism does not extend to other groups and diminish citizens' trust in them. According to a survey the Taiwan FactCheck Center conducted in 2022, 54% of citizens use fact-checking channels to verify suspected fake news, and 76% of citizens remind their friends of the existence of certain types of fake news.[10] Since these organizations operate independently and are bipartisan, they gain trust within society more easily than the government does.

It is also worth mentioning civil society's use of bots in the debunking process. For example, more than 200,000 people have used the MyGoPen Robot to push newly debunked pages through the most popular peer-to-peer chat apps (such as LINE). Bots have also been employed to automatically analyze and debunk suspicious messages using data collected from civil society organizations. Some bots can be added to group chats to automatically pump out debunking messages when fake news is detected. These bots can also detect videos and images, which have become popular tools for disinformation campaigns.

BEST PRACTICES AND POLICY RECOMMENDATIONS

Civil society and the DCT do not collaborate with each other in the debunking process. This is another factor that helps maintain the public's trust in civil society groups, as the groups cannot be seen as channels for spreading possible propaganda. However, there are several challenges associated with Taiwan's model of combatting disinformation.

First, there is no common definition of — and approach to identifying — cognitive warfare. The information flow from China to Taiwan does not often include fake news, but rather conspiracy theories or opinions and perspectives that are difficult to debunk. The only way to combat these types of disinformation is to reveal the Chinese accounts' behavior rather than focus only on the messages. For instance, the Doublethink Lab has worked on cyber army issues for years, but China often disseminates whataboutism messages such as "the Taiwanese government also has the cyber army" and "the U.S. is the one that uses a cyber army."[11] Furthermore, the statements of opposition parties in Taiwan, such as the Nationalist Party and the Taiwan People's Party, are sometimes aligned with Chinese messages, which creates confusion. In this way, it has become extremely difficult for the government or nonprofit organizations to highlight possible incidents of cognitive warfare without offending opposition parties. To better approach this serious but inadequately addressed issue, civil society groups and Taiwan's legislative bodies should jointly develop a clear, legal definition of cognitive warfare. As stated above, disinformation operations involving conspiracy theories and money- and human-driven messages have not been fully debated and discussed. Taiwan's version of the U.S. Foreign Agents Registration Act has also failed to pass. To focus on the behavior of actors rather than the messages, what counts as "illegal behavioral patterns" should be clearly outlined in a common definition of cognitive warfare. For example, if Taiwanese professors are spreading pro-China messages, the conclusion about whether the professors are engaging in cognitive warfare should be based on predetermined standards: Did the professors receive interest or sign a contract with China? Did the professors agree to engage in inauthentic behavior to harm society, for instance by asking students not to discuss things that happened in Hong Kong? With such standards set, the behavior could be confidently identified as cognitive warfare. A public hearing or strict evidence-based accusation and attribution is necessary, and legal measures is the way to reach this end.

Second, the money flow that entices citizens to spread pro-China messages has not been stemmed. To be sure, in a democratic world, it is impossible to totally restrict these kinds of investments, as most speech falls into the category of free speech. The best way to combat the money flow is to (1) establish clear restrictions for Chinese investments within each industry (for example, less than 50% investment) and (2) reveal the flow of money from Chinese party or

state actors to Taiwanese individuals or organizations. Transparency is essential, and this strategy fits the spirit of democracy.

Restrictions on content or the punishment of actors will not fix the problem. Criminal punishment not only creates division but also requires hard-to-collect evidence needed for convictions. While Taiwan's anti-infiltration law passed in 2019 may be serving as a deterrence, no cases have been prosecuted under this law yet, likely because the evidence is too difficult to gather.

Third, while the human flow of disinformation might be the most serious concern, it would go against democratic norms of free speech and individual liberties to punish people for their ideological beliefs. Therefore, revealing what the United Front Work Department (UFWD) and other actors do in each country might be the only way to counter the human flow of information. For example, the Taiwan Handout website, operated by anonymous writers, attempts to reveal certain forms of infiltration without exacting punishment.[12] In 2019, the website revealed a connection between a certain political Facebook FanPage in Taiwan with the UFWD, and in turn, sparked a discussion about Chinese interference before the 2020 presidential election.[13]

A local workshop hosted by two organizations, Fakenews Cleaner and Chat for Taiwan, engages citizens who are familiar with digital platforms and messaging services but are often not tech savvy enough to spot or judge potential disinformation. Efforts like this one could help the public easily identify and understand harmful disinformation on social media platforms and rumors within local communities. Already, since 2018, Fake News Cleaner has hosted more than 500 activities across Taiwan.[14]

Fourth, since Chinese information operations are organized by multiple government departments, they need to be countered in a systematic and holistic way. Cross-national workshops and initiatives can help to effectively combat these operations. Doublethink Lab and the Taiwan FactCheck Center have hosted several international workshops since 2019. During the invasion of Ukraine, both Fake News Cleaner and Chat for Taiwan have been utilizing global networks to join the international debunking of disinformation campaigns and share knowledge with concerned partners who face similar attacks.

Lastly, in addition to establishing clear, legal definitions and standards and enhancing transparency, the government and civil society must respond to conspiracy theories in a positive and constructive way and avoid delivering punishment-like and negative messages. For example, there was once a rumor that the Taiwanese government had collected a lot of private information during the COVID-19 pandemic and was going to use the data clandestinely.[15] The Taiwan Centers for Disease Control quickly debunked this information, merely saying that the rumor was fake news. The problem is that such limited responses can create further distrust of people and agencies who share debunking messages. A positive and constructive response would have been, for example, "we recognize the nature of why this rumor was spread — because the mechanism of protecting privacy is not transparent. Therefore, we will soon establish a committee to oversee data and make sure it is deleted every three months. Please rest assured that we will keep improving our processes." In this way, the whole society could create trust and easily stop disinformation from spreading.

REFERENCES

1 Varieties of Democracy (V-Dem), https://www.v-dem.net/.

2 Puma Shen, "The Chinese Cognitive Warfare Model: The 2020 Taiwan Election," *Prospect Quarterly* 22, no. 1 (January 2021): 1-65, https://www.pf.org.tw/en/pfen/37-8137.html.

3 Puma Shen, "How China Initiates Information Operations Against Taiwan," *Taiwan Strategists* 12 (2021): 19-34.

4 Puma Shen, et al., "Deafening Whisper," Medium, October 24, 2020, https://medium.com/doublethinklab/deafening-whispers-f9b1d773f6cd.

5 Austin Wang, "中國Youtube假主播罷Q全面啟動" [Fake Chinese news anchors on Youtube have started to appear], 思想坦克 [Voice Tank], October 14, 2021, https://voicettank.org/%E4%B8%AD%E5%9C%8Byoutube%E5%81%87%E4%B8%BB%E6%92%AD%E7%BD%B7q%E5%85%A8%E9%9D%A2%E5%95%9F%E5%8B%95/.

6 Puma Shen, "The Chinese Cognitive Warfare Model: The 2020 Taiwan Election"; William Kung, Haohsing Ke, Chihhsin Liu, and ChiaYu Hsu, "Uncovering the Money and China Factor Behind 'Mission' — Taiwan's Most Controversial Content Farm," The Reporter, December 25, 2019, https://www.twreporter.org/a/information-warfare-business-content-farm-mission-english.

7 Chen Yanyu [陳彥宇], "蘇內閣向在野黨宣戰　政院幕僚被抓包製作「網軍圖卡」" [The Executive Yuan was caught providing memes to cyber armies], Up Media, November 3, 2020, https://www.upmedia.mg/news_info.php?Type=1&SerialNo=99453.

8 Shih-Shiuan Kao, "Taiwan's Response to Disinformation A Model for Coordination to Counter a Complicated Threat," NBR, September 16, 2021, https://www.nbr.org/publication/taiwans-response-to-disinformation-a-model-for-coordination-to-counter-a-complicated-threat/.

9 Ibid.

10 "Annual FactCheck Report," (Taipei: Taiwan FactCheck Center, 2022), https://tfc-taiwan.org.tw/.

11 Shen, et al., "Deafening Whisper."

12 See https://taiwanhandout.org/.

13 畢厚德 [Bi Houde] "挺韓大將徐正文遊走兩岸的政治身份"[Xu Zhengwen, a general who supports South Korea, roams the political identity of both sides of the strait], TaiwanHandout, October 18, 2019, https://taiwanhandout.org/archives/427.

14 Jordyn Haime, "Taiwan's amateur fact-checkers wage war on fake news from China," Al Jazeera, September 19, 2022, https://www.aljazeera.com/economy/2022/9/19/taiwan.

15 "網傳「簡訊實聯制監控人民行蹤」 指揮中心：不實訊息勿轉傳以免觸法" [Online "SMS real-time joint system to monitor people's whereabouts" command center: Do not repost false information to avoid breaking the law], Ministry of Health and Welfare of Taiwan, May 23, 2021. https://www.mohw.gov.tw/cp-17-60900-1.html.

DISINFORMATION IN THAILAND

AIM SINPENG

DEFINING THE CHALLENGE

The use and misuse of digital technologies has upended the relationship between citizen and state, abetted oppressive governments, and posed immediate and long-term threats to democracy. More than 70% of the world's population lives in countries whose governments employ at least one form of cyber repression.[1] Disinformation, in particular, has become an increasingly common tool to undermine online freedom and intervene in the affairs of a foreign country. Disinformation campaigns to control and manipulate information in Thailand have been proliferating alongside internet and social media usage. The Freedom House and V-Dem has ranked Thailand's internet environments as illiberal for nearly a decade, beginning with a military coup in 2014.[2] Similar to the rest of Asia, the sources of disinformation are both domestic and foreign and involve state and nonstate actors. To understand Thailand's problem, it is important to recognize that disinformation is embedded in an autocratic and repressive media ecosystem, where media organizations as well as ordinary people are routinely censored, monitored, and occasionally punished for actions deemed to threaten the state's peace and order.

What is unique about Thailand's disinformation challenge is the political landscape from which disinformation emerges. Despite its highly restrictive digital environment and draconian laws against regime critics, Thailand is the most protest-prone autocracy in the world.[3] The country's cyber structures, laws, and institutions designed specifically to thwart and punish political dissent have thus failed spectacularly to dampen the opposition's activism and quell protests.[4] Fortunately, this means that the global proliferation of disinformation and cyber repression might not spell the end of digital activism.

Yet, disinformation has undoubtedly undermined pro-democracy activism and strengthened autocratic governance in Thailand. With coups in 2006 and 2014, the country has been marred by deep polarization between status-quo-seeking conservatives, who desire stability from traditional power brokers (for example, the military, monarchy, and bureaucracy), and pro-democracy reformists, who desire drastic political change. This deeply entrenched political division has provided fertile ground for disinformation to thrive, as each side uses the tactic to embolden their status and discredit their opponents. Adding to the mix are geopolitical and economic factors that introduce new kinds of disinformation, further muddying the already murky information environment.

There are three key drivers of disinformation in Thailand: political, institutional, and economic.

POLITICAL DRIVERS OF DISINFORMATION

These drivers largely come from domestic sources, involving both state and nonstate actors. In Thailand's polarized political landscape, government agencies, nongovernmental organizations, political organizations, and commercial enterprises have all been implicated in employing disinformation tactics to make political gains.[5] However, state and nonstate actors bear different risks and costs when producing disinformation. The cost of employing disinformation is lower for state actors. In an

authoritarian state like Thailand, state agencies, especially politically powerful ones like the military, can be more confident that their activities will not be repressed or punished. While on the contrary, opposition political groups employing a similar tactic against the Thai state face a significantly much higher cost: They could be sued or imprisoned and their campaigns could be censored or manipulated.

Civil society actors groups have used disinformation campaigns to support democratically elected governments or to pave the way to a democratic breakdown. For example, the People's Alliance for Democracy (PAD), known locally as the "yellow shirts," mounted a powerful conspiracy theory, the Finland Plot, to dislodge the democratically elected government of Thaksin Shinawatra in 2006.[6] Leveraging satellite TV, street rallies, radio, newspapers, and the internet, the PAD and its allies campaigned against Thaksin, accusing him of plotting to turn Thailand into a republic. Subsequently, social media became a major tool for political participation both in support of and opposition to democratically elected governments. The Facebook-fueled political protests of the People's Democratic Reform Committee, the PAD's successor movement, highlight the importance of social media as a platform to facilitate anti-democratic mobilization. Notably, the committee's protests brought to the fore how indispensable social media is in building narratives, driving discourses, and recruiting and mobilizing a support base to achieve specific political gains, no matter how radical the ideas.

INSTITUTIONAL DRIVERS OF DISINFORMATION

These drivers facilitate disinformation and strengthen institutional mechanisms for authoritarian resilience. In Thailand, the 2007 Computer-Related Crime Act (CCA) and its 2017 amendments lay the institutional foundation for disinformation to emerge and thrive, as they give state agencies greater power to control information. The ambiguity of Thailand's cyber laws prompted a local online newspaper, Prachatai, to publish information that advises readers on how to avoid violating the CCA. In turn, Thai authorities interrogated the journalist responsible for the article for a possible computer crime. Affording the state even more control, the country's cyber laws are often used alongside Article 112 of the Penal Code, which makes it illegal to defame, insult, or threaten the monarchy. A 69-year-old woman was initially sentenced to prison for 87 years for sharing video clips deemed threatening to the monarchy.[7] This deadly dose of opaque cyber regulations on the one hand and an illiberal, authoritarian political regime on the other has made the Thai cyberspace one of the most restricted spaces in Asia.

The military, in particular, sees digital technologies as an integral part of its broader information warfare strategy. Its early efforts to control information were focused on overt forms of control such as censoring, blocking, filtering, and arresting regime critics. It was not until the late 2010s that social media was seen as a platform for bolstering popular support for the military and a space for public opinion manipulation. This shift from hard forms of censorship to online manipulation follows the global trend in which social media is increasingly used, particularly by authoritarian regimes, to monitor, manipulate, and marginalize critical voices. The Thai military likely fears the formation of underground groups that seek to subvert the Thai nation, particularly to overthrow the monarchy.

On October 8, 2020, Twitter announced the takedown of 926 accounts targeting Thai Twitter users in a domestic information operation. Twitter attributed these accounts to the Royal Thai Army and shared the accounts with the Stanford Internet Observatory on September 24, 2020.[8] This was the first time Twitter included activity originating in Thailand in its state-backed information operations archive. However, it is not the first time the military has been accused of running information operations. In February 2020, the Future Forward Party accused the prime minister and minister of defense of conducting information operations to attack opposition candidates on Facebook.[9] A series of leaked documents and interviews with a whistleblower from the Thai army in early 2020 support this account

and suggest that the information operations began prior to the 2019 elections. The whistleblower who came forward was disillusioned that taxpayer dollars were used to sow discord and hatred online. The alleged operation on Facebook supported the Thai army, commented negatively on opposition members' Facebook pages, and spread false information and graphics attacking political opposition members. Although there is no indication that the Twitter takedown is linked to the Facebook information operation previously reported, the takedown dataset reveals similar tactics and aims, especially a reliance on posts that promote the Thai army and critique opposition party members. The Twitter takedown case in Thailand, however, did not reveal surprising new information. Civil society and opposition groups suspected these state-backed disinformation operations months before the platform released its takedown notice.

ECONOMIC DRIVERS OF DISINFORMATION

These drivers largely stem from the growing influence of China in Thailand's information landscape. Its influence has been growing in two main ways. First, Chinese firms have been increasing their presence in the Thai media, telecom, and technology markets. While Thailand is no stranger to Chinese foreign investment, the takeover of struggling Thai media organizations and the expansion of China's state-run media organization are worrisome trends. Chinese-run media organizations in Thailand have introduced new forms of information control and manipulation to shape narratives on sensitive topics relating to China. The growing power of Chinese media organizations overseas has been regarded as the widening and deepening of digital authoritarianism. Chinese surveillance software is being exported to other countries in its sphere of influence.[10] Xinhua Thai News Service, a Thai offshoot of China's state-run Xinhua, delivers news on Hong Kong that is in line with the Chinese Communist Party's approved narratives. Sanook News, taken over by the Chinese tech giant Tencent, delivers more nuanced coverage of news on Hong Kong protests.

Second, Thailand is a major adopter of Chinese artificial intelligence (AI) surveillance technologies, which have been used in combination with other spyware to attack the political opposition. Like many countries around the world and particularly authoritarian regimes, Thailand's growing use of China's AI, especially facial recognition software, raises concerns over privacy and ethics.[11] The Australian Strategic Policy Institute's maps of Chinese tech giants in Thailand show that an increasing number of China's technologies are being used across sectors in Thailand, from banking to health care to public security.[12] A more widespread adoption of China's surveillance technology could further induce disinformation and make mass surveillance a "new normal."

ASSESSING POLICIES AND PRACTICES

The 2007 CCA, brought on by the 2006 military coup, was Thailand's first cyber law. It banned the distribution of "false information" in computer networks, which was believed to be an attempt to stop cybercrimes like hacking. But the CCA has been used in conjunction with libel charges to prosecute speech deemed as a threat to national security, peace, order, and implicitly, the monarchy. In 2017, amendments to the CCA added the terms "distorted" and "partially distorted" computer information, which essentially extended the ambiguity of the law and how it could be applied to silence regime critics. According to Thai Lawyers for Human Rights, government agencies and large corporations have since regularly used the CCA to facilitate strategic lawsuits against public participation in criticism, comment, or action on issues of public interest).[13] Changes to the CCA have also given the state greater authority to exercise censorship online, stifle free speech, and thwart critical voices. Online commentary against the CCA can now constitute false information and lead to prosecution Additionally, the Thai army has set up its own Army Cyber Center in tandem with the already existing Technology Crime Suppression Division. These organizations seem to have a wide scope to monitor dissent and protect the monarchy and to interpret what information could be false, partially false, distorted, and

partially distorted. Shortly after the organizations were established, hundreds of websites were shut down on the grounds that they could disturb the quality of public life.

The most consequential institution set up to combat disinformation is the Anti-Fake News Center (AFNC), established in 2019 by the Ministry of Digital Economy and Society.[14] Thailand does not have an independent fact-checking organization (it is only part of the AFP-affiliated fact-checking initiative), so the AFNC seeks to fill this void, but it is a wholly governmental effort and thus lacks independence from the state. The AFNC was designed to combat false content and was regularly used to counter misinformation and conspiracy theories relating to COVID-19. Also among its mandate, however, is the review of content that could disturb the peace and order of the nation. As a state-run agency, the AFNC engages in countering false information through the dissemination of corrective information.[15] But opposition parties have accused the government of using the AFNC only to investigate disinformation campaigns against the incumbent.[16]

BEST PRACTICES AND POLICY RECOMMENDATIONS

Thailand's best defense against disinformation will come from the ground up. Strengthening the networks of grassroots groups and individuals who understand and demand digital rights is the best antidote against a domineering, illiberal, and autocratic internet regime. While not all digital rights activism is successful, such collective opposition to state initiatives that could increase information control and opportunities for manipulation is instrumental in signalling to the incumbent that their actions are unacceptable.

The most effective grassroots effort in Thailand to fight against the state's crackdown on internet freedom was the "anti-single gateway" campaign in 2015. The military junta sought to consolidate internet traffic through the creation of a single, harmonized, government-controlled gateway that would permit additional policing of information flows. Internet advocacy groups created online petitions on change.org that elicited more than 500,000 signatures and much heated conversations across a number of Thai Web board communities. Another online group was created on Facebook, พลเมืองต่อต้าน Single Gateway เพื่อเสรีภาพและความยุติธรรม ("Citizens against the Single Gateway for Freedom and Justice"), in retaliation against the state's plan to tighten control over the Thai cyberspace. This Facebook group received more than 200,000 likes and similarly generated grassroots pressure on the government's controversial plan.[17] Eventually, the Thai government backed off from the single gateway proposal.

The Thai case has shown the importance of identifying and understanding disinformation campaigns that emerged within the state. Specifically, disinformation operations organised by the state to attack political opposition groups and manipulate public opinion toward public institutions.

Lessons learned in studying Thailand's state-sponsored disinformation operations provide the following policy recommendations:

- It is challenging to prove the existence of disinformation campaigns without the cooperation of tech platforms. There is very limited public access to data that could provide hard evidence of disinformation campaigns and reveal their nature and attributes. Tech platforms need to cooperate more with Thai internet and social media users to identify disinformation, particularly if the content comes from the state. Platforms can label state-run disinformation accounts, shut down accounts that spread false information more efficiently, and provide resources in the Thai language to help users identify disinformation.
- Civil society and opposition groups are often at the front line of state-backed disinformation operations, as they are likely targets and victims of such actions. Because of these groups' vulnerability to disinformation, tech platforms and civil society networks should provide them with training on how to manage such problems and what resources are available to strengthen their call for investigation.
- Grassroots digital literacy campaigns and social technologies that focus on raising awareness of disinformation, misinformation,

and propaganda are crucial to building public immunity against disinformation. A notable effort is the 606 Fake News Game developed by Opendream, a Thai social enterprise, which has been shown to improve players' ability to spot false information[18]. The game was designed to increase Thai youths' capability to identify false information, measured by a pre- versus post-game knowledge test. The game's success demonstrates how gaming can be used to reduce young people's vulnerability to false information.

- Disinformation from foreign actors remains challenging to identify systematically, as it takes many different forms and comes through various vehicles such as foreign investment. To enhance their ability to detect and map foreign interferences in the information environment, Thai civil society, media organizations, and academic institutions need to strengthen their capacity for investigative and data journalism. They can do this by prioritising digital analytic skills, such as participating in free online trainings offered by the Google News Initiative Training Center and Thailand Data Journalism Network.

REFERENCES

1 "Freedom on the Net 2021: Thailand," Freedom House, https://freedomhouse.org/country/thailand/freedom-net/2021.

2 "Digital Society Project," V-Dem, http://digitalsocietyproject.org/.

3 Sinpeng, Aim. *Opposing Democracy in the Digital Age: The Yellow Shirts in Thailand*. University of Michigan Press, 2021.

4 Aim Sinpeng, "Digital media, political authoritarianism, and Internet controls in Southeast Asia," *Media, Culture & Society* 42, no. 1 (November 2019): 25-39, https://journals.sagepub.com/doi/10.1177/0163443719884052.

5 Pavin Chachavalpongpun, "Nationhood in the Cloud: Cyber Sovereignty in Thailand." *Asian Studies Review* (2022), https://doi.org/10.1080/10357823.2022.2109591.

6 "ชำแหละปฏิญญาฟินแลนด์" [Dissecting the Finland plot], Manager Online, May 25, 2006, https://mgronline.com/daily/detail/9490000068410.

7 "พิพากษาคุก 'อัญชัญ' คดี 112 แชร์คลิปยูทูบ หมิ่นสถาบัน 29 ปี 174 เดือน" [Judges handed 'Anchan' the article 112 case for sharing lese majesty YouTube clips 29 years 174 months], Matichon Online, January 19, 2021, https://www.matichon.co.th/local/crime/news_2536045.

8 Aim Sinpeng, Josh Goldstein, Daniel Bush, Ross Ewald and Jennifer John. "Cheerleading Without Fans: A Low-Impact Domestic Information Operation by the Royal Thai Army," (Stanford: Stanford Internet Observatory, October 2020), https://cyber.fsi.stanford.edu/io/news/twitter-takedown-october-2020.

9 "วิโรจน์ ลักขณาอดิศร: เด็ดมาก! เปิดขบวนการ IO ใช้ภาษีคนไทยทำร้ายคนไทยด้วยกันเอง" [Wiroj Lakana-Adisorn: Great job revealing IO mission using citizens' taxes to hurt Thai people], Future Forward YouTube Channel, February 26, 2020, https://www.youtube.com/watch?v=qhnlhXZkRx8.

10 Adrian Shahbaz, "The Rise of Digital Authoritarianism: Freedom on the Net 2018," (Washington, DC, and New York: Freedom House, October 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

11 Sheena Chestnut Greitens, "Dealing with demand for China's global surveillance exports," (Washington, DC: The Brookings Institution, April 2020), https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/.

12 "Mapping China's Tech Giants," Australian Strategic Policy Institute, https://chinatechmap.aspi.org.au/#/homepage.

13 "Freedom on the Net 2021: Thailand," Freedom House, https://freedomhouse.org/country/thailand/freedom-net/2021.

14 Anti-Fake News Center Thailand, Ministry of Digital Economy and Society, https://www.antifakenewscenter.com/.

15 Janjira Sombatpoonsiri, "Labelling Fake News: The Politics of Regulating Disinformation in Thailand," *ISEAS Perspective* no. 34 (April 2022), https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-34-labelling-fake-news-the-politics-of-regulating-disinformation-in-thailand-by-janjira-sombatpoonsiri/.

16 "ส.ส.ก้าวไกล อภิปรายเหตุที่ไม่ควรให้งบ 'ศูนย์ต่อต้านข่าวปลอม' - เปิดงบซ่อมถนนยังคงทุ่มให้ 'บุรีรัมย์' นำโด่ง" [Move Forward Party MPs argued there should be no budget for the Anti-Fake News Center. The proposed budget for building roads in Buriram would remain], Prachatai Online, August 19, 2022, https://prachatai.com/journal/2022/08/100100.

17 "พลเมืองต่อต้าน Single Gateway เพื่อเสรีภาพและความยุติธรรม #opsinglegateway [Citizens against Single Gateway for Liberty and Justice], Facebook group, https://www.facebook.com/OpSingleGateway/.

18 "606 Fake News Game," OpenDream, https://www.opendream.co.th/project/606-fakenews-game.