How China Initiates Information Operations Against Taiwan

Puma Shen

Assistant Professor,
Graduate School of Criminology, National Taipei University

Abstract

China's information operation tactics have become a threat to the world, especially in the case of Taiwan. In addition to cyber-attacks, the disinformation campaigns initiated by China have expanded in the last five years. Traditionally, researchers utilize the cyber kill chain model to explain the dissemination of disinformation. However, the motivations and echo-systems of this model have seldom been explored. This article discusses the concept of 3Is: direct information operations initiated by Chinese actors, indirect investments toward Taiwanese local citizens, and an ideology-driven approach that weaponizes people in the market of disinformation. This categorization reveals the adversaries within the industry of production, their motivation, and their effectiveness. I further argue that, using COVID-19 narratives as an example, the 3Is collaboration indicates that China is capable of doing serious harm to foreign countries.

Keywords: 3Is, Information Operation, Investment, Propaganda, Ideology

I. Introduction

Chinese influence shapes the world we live in. Taiwan, as a testing ground for China information operation, faces all forms of attack. To understand Chinese information operations, it is crucial to not categorize these attacks in a traditional way. Unlike Russian operations, Chinese information operations are either centralized or decentralized. To explain this, the command of the Chinese Communist Party (CCP) might be centralized, but the operators have their own capacity to initiate attacks, and these attacks are often decentralized since operators seldom collaborate with each other. Operators try to find niches they can fit into, and once they find a topic that

suits the CCP's propaganda and purpose, they try hard to apply for government funding, initiate an attack, and revise their strategy when the attack is voided.

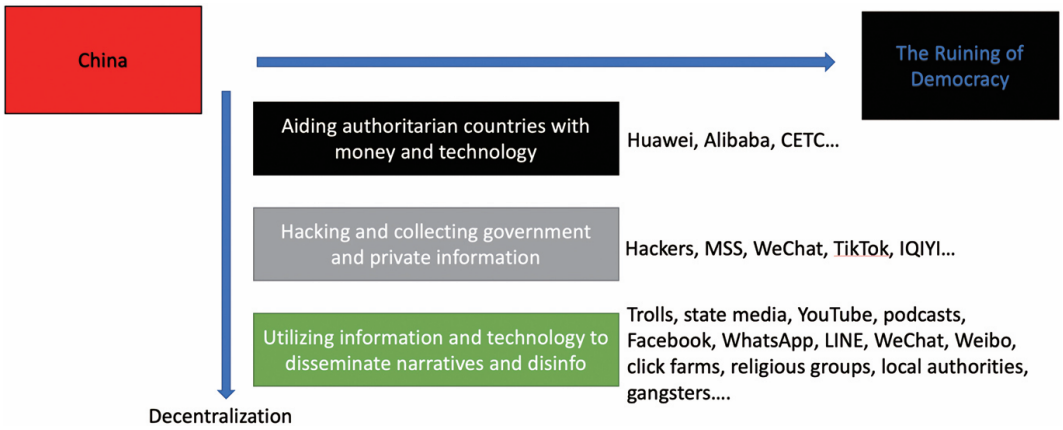

Figure 1. The Decentralization of Chinese Information Operations

Source: Compiled by the author.

To achieve the goal of disrupting Taiwanese society, several steps must be undertaken. First, China can hack into governmental systems, stealing and collecting information to serve its agenda. Hackers from China have launched persistent attacks around the world, targeting Taiwan in particular. These attacks are centralized. However, China can also utilize private companies—most of them with party committees, such as WeChat and GTCOM—to collect information. Hundreds of apps like these can serve this purpose, collecting information that can be utilized for big data analysis. With this collected info, it is much easier for China to do the profiling—to determine which groups of people are more vulnerable than others. Preliminary evidence indicates that some disinformation has only been spread in certain counties/provinces in Taiwan, using the aforementioned tailoring.

Second, China can exploit the technology it has and the information it gathers to launch information warfare. Companies like WuWei technology operated online Facebook psychological tests and established content farm websites to spread disinformation to Taiwanese targeted groups in 2017. This disinformation was not only spread online, but also offline, with numerous groups involved, such as religious groups, gangsters, local parties, and local elites. These attacks are decentralized and hard to detect, ultimately crushing democracy.

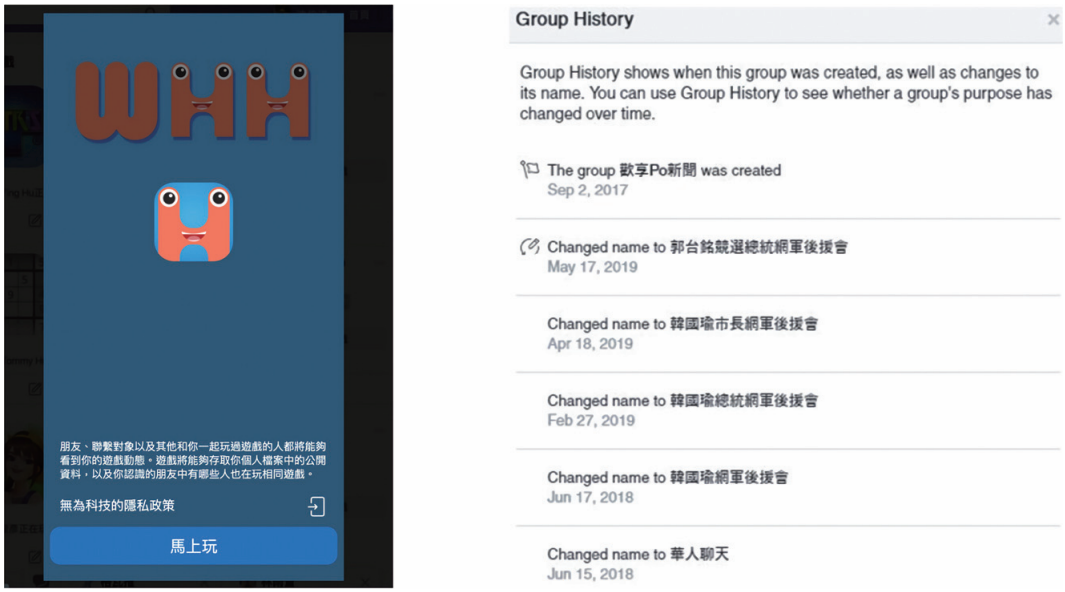

Figure 2. The Psychological Tests and Facebook Groups Created by Chinese Companies

Source: Compiled by the author.

Therefore, in understanding the Chinese strategy of initiating information operations, one should first realize that multiple departments, companies, and groups are involved. The propaganda department is just one of the players focused on setting the key theme, but other players in the field, whether they agree with the Propaganda department or not, might initiate their own attacks to serve their own purposes (e.g., to distract from internal public attention, initiate factional struggle, or simply counter anti-CCP messages around the world). The role of United Front Work Department (UFWD) is the key here since this very department, along with the Chinese People's Political Consultative Conference (CPPCC), tries to unify all kinds of attacks.[1] In order to better understand the Chinese style of information operations, I propose the idea of 3Is, as discussed below.

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

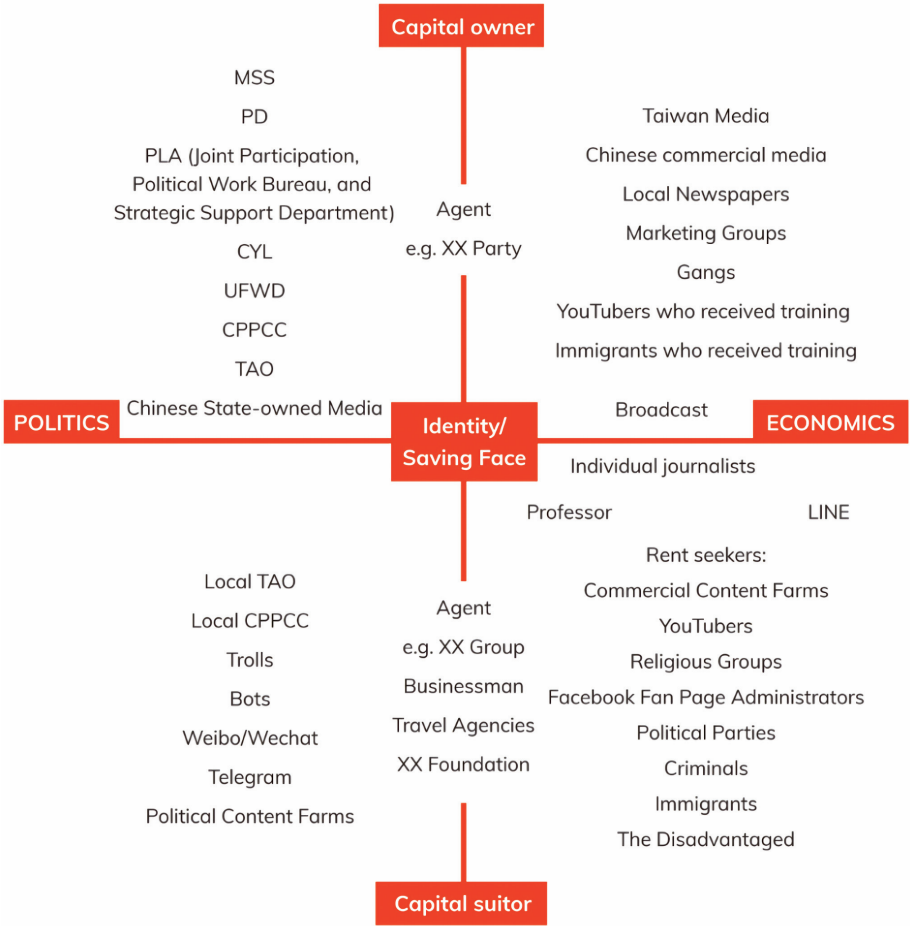

Figure 3. Players Involved in Disinformation Campaigns

Source: Compiled by the author.

II. The Diamond Model

The goal of a disinformation campaign (or information warfare) is to disturb a targeted society. To accomplish this, disinformation has to have some basis in fact or correspond to a widely accepted belief. It should fit with prevailing narratives in the target population, play to people's prejudices, and nurture innate suspicions. To be credible, it needs to appear to come from trusted sources—preferably at some distance from where it actually originated. To have an impact, it needs to be spread to a certain scope and repeated regularly. The reiteration of the same news story—even if it is invented entirely—will eventually seep into people's minds and gain a sense of veracity.

The ultimate sign of success is when someone comes to believe what China wants them to believe but thinks they came to the conclusion by themselves. For example, the Russian style of disinformation campaigns used to focus on fostering political divisions, eroding trust in authorities, encouraging partisanship, and nurturing anger towards U.S. and European political systems, using gun issues, vaccines, and racial inequality as the main topics; in Taiwan, any inner conflicts within the parties, labor issues, LGBTQ marriage, and energy debates can be utilized as weapons to erode public trust towards society and government institutions.

Topics	Strategies	Emotions	Biases	Nodes
Military Diplomacy Infrastructure Economy Disease Political figures Industry Health LGBT Generation alienation Immigration Nuclear energy U.S.-China relations Labor management Transitional justice Identity-institution Identity-ethic group Identity-culture	Distorting Dismissing Narrowing Amplifying Extending Dismaying Distracting Repeating "If" Dichotomy Hypocrisy Generalization Slippery slope Novelty Conspiracy	Hope Love Dislike Fear Anger Anxiety Hate Sympathy Surprise	Availability bias Confirmation bias Resonance Cognitive dissonance Trust dilution Neutralization Trusting the source Rather believe	State media in both countries Weibo Podcasts Content farms Cyber forces Trolls YouTube Marketing co. Broadcasts Facebook PTT, Dcard Political talk shows News Magazines Local elites Religious groups Professors, schools Travel agencies Local parties Chinese immigrants Chinese students Retiring groups Foundations Businessmen

Figure 4. Topics, Strategies, Emotions, Biases and Nodes Within the Disinformation Campaign

Source: Compiled by the author.

The means to reach the ends vary. To select a controversial topic is one thing; to successfully reach the target audience is another. China can easily select the target audience within the UFWD network by spreading offline rumors, but it can also utilize online tools to specifically target the groups of people vulnerable to Chinese disinformation. The Search Engine Manipulation Effect (SEME) has been observed in Taiwan from 2018 to 2020,[2] and the content farm (click farm) business was also established by Chinese businessmen to disseminate pro-China messages around the

2.〈誰最愛 Google 韓國瑜？去年台灣排 16 這國第一名〉, *Liberty Times*, December 4, 2019, <https://news.ltn.com.tw/news/politics/breakingnews/2998826>; 〈Google 搜尋亂碼卻跳出「陳菊 善款」〉, *Mirror Media*, June 10, 2020, <https://www.mirrormedia.mg/story/20200610edi001/>.

world.[3] Some messages targeted polarized groups, but some targeted apolitical citizens who had no idea about Chinese information operations. The bot networks related to China can easily amplify the elected topic, in turn shifting the ideology.

Thus, information operations require the attacker, a selected topic, a network and channel that reach the targets, and victims who believe in certain messages to all function together. This kind of disinformation campaign shares many characteristics with a traditional cyber espionage operations. Consequently, the Diamond Model used in cyber threat hunting, which stresses the adversary, infrastructure, capability, and victim, could replace the cyber-kill chain with the disinformation chain.

A rough mapping of core features in a Chinese information operation onto the Diamond Model is as follows: 1. Adversary: 311 Base/Strategic Support Force (SSF), Network Systems Department (NSD)/SSF, Ministry of State Security (MSS), Ministry of Public Security (MPS), People's Armed Police (PAP), Political Work Department Liaison Department/Central Military Commission (CMC), UFWD, civilian contractors, and other private groups; 2. Infrastructure: C2, bot network, IPs, emails, phone numbers, websites, real/fake accounts on social media, Chinese Diaspora, professors, businessmen, clan associations, religious groups, and gangsters; 3. Capability: content creation, content selection, and media surveillance; 4. Victims: unwitting media outlets both online and offline, audiences from various social media platforms, private messenger groups, and geographical areas surrounding Taiwan.

Within this framework, there are several ways to categorize Chinese information operations. For example, by categorizing the operating infrastructure, one could say that China is initiating content farm attacks, SEO attacks, media attacks, and TikTok attacks. By categorizing the operators, one could argue that Taiwan is facing SSF attacks or UFWD attacks. However, this lens does not allow us to understand Chinese information operations, and China's intentions and motivations are missing. The other way to assess this phenomenon is to analyze the content China provides through its official media and related entities, but this methodology can easily ignore the offline rumors spread by local collaborators and miss the fake posts provided by cyber warriors

3.〈打不死的內容農場——揭開「密訊」背後操盤手和中國因素〉, *The Reporter*, December 26, 2019, <https://www.twreporter.org/a/information-warfare-business-content-farm-mission>.

or patriots (e.g., some cyber warriors pretend to be Falun Gong supporters and spread low-end disinformation in order to ruin Falun Gong's reputation worldwide).

To avoid these loopholes, one should categorize Chinese attacks from the bottom up, deducing types of attacks from the collected data (online archives including Facebook, Instagram, boards, WeChat, and Weibo; offline rumors from local citizens), further providing a rationale. In this way, I have provided three different kinds of attacks from China against Taiwan; all three share different adversaries, infrastructure, capabilities, and victims. The idea of the 3Is—direct information manipulation, indirect investment, and an ideology-driven approach—are discussed below.

III. The 3Is Concept

With collected online and offline rumors, it was difficult in the beginning to attribute disinformation attacks to the Chinese government. However, since different departments have different topics of interest and are using different resources, it is possible to infer who the possible adversaries are. First, I will introduce the direct information manipulation occurring in China and the indirect investment that leads to the establishment of the disinformation market. In the end, I will illustrate the ideology-driven approach that stands out as a Chinese style of information operation.

1. Direct Information Manipulation: Information Flow

Direct information manipulation shares characteristics: all adversaries are foreigners (not limited to Chinese), and there are three that vary in scale and intensity.

(1) High-level information manipulation, usually through the Propaganda Department along with the execution of CPPCC and UFWD, will set the key theme. The information manipulated by high-level departments or committees can be observed through state media or officials' Twitter accounts. Although sometimes using low-end conspiracy theories during the pandemic, usually they only set up the key tone —for example, which topic to select—every several weeks.

(2) There is low-level information manipulation through the trolls and patriots; the so-called "little pinks" or cyber warriors are capable of spreading disinformation

as well. Most information spread in this way involves low-end fake news and seldom does harm to society. These parties often flood social media comment areas or simply use bot networks to share messages. This kind of disinformation often incites anti-China feelings among citizens and is the least worrisome kind of disinformation to tackle. The People's Armed Police may be involved in these activities, but it focuses more on inner stability maintenance than on disinformation campaigns worldwide.

(3) Connected-level information operations: researchers who often focus on high-level propaganda or 50-cent low-level party activities, but what really does harm to Taiwanese society is the connected-level information operation, which is derived from China-controlled content farms. Articles from content farms consist of conspiracy theories, biased reports, and normal reports with biased titles. These websites often share entertainment, fortune-telling messages, or cute animals that attract Taiwanese citizens and then spread biased reports that denounce any other countries but China. These reports are mostly narratives that connect the key theme set up by propaganda and the low-level rumors spread by little pinks. They are usually not forms of fake news that can be easily debunked, and they compel readers to accept certain ideologies.

The impact of connected-level information, however, is not guaranteed. According to the diamond model explained above, the adversary should make sure information is "delivered." To accomplish this, we must investigate the infrastructure.

Figure 5. The Network that Spread Disinformation in the Kansai Airport Incident

Source: The author collected from Weibo.

First, the 50-cent party—or the cyber police, if they are close to the central or local government—might receive orders to disseminate those articles instead of low-end fake news; the Communist Youth League, often involved in inciting little pink activities, is also capable of connecting ideologies and disinformation in the cross-posting of content farm articles on Facebook or Twitter. Recently, I also specified Facebook groups established by China and Cambodia users, first-post articles that are pro-DPP, and further dissemination of content farm articles that denounce Taiwan-made vaccines.

The advanced model of content farms article cross-posting is the utilization of an algorithm on YouTube that allows content to reach more audiences. Starting in 2019, China established several content farm channels (in addition to state media channels) to establish the connection between ideology and disinformation. These

channels can upload up to four videos daily, and each of them has more than 10,000 subscribers. The virtual host of the video will read content farm articles with AI-voice generators that resemble Taiwanese accents, using large size subtitles in traditional Chinese to make sure elder generations can consume the messages; these recordings can appear often on YouTube if one clicks videos of cute animals and fortune-telling articles. Recently, eight channels that have been established to denounce the Taiwanese government have uploaded 2000+ videos within a period of six months, receiving 30 million view counts.

To sum up, the first "I" is usually overt, and it can be truly effective and harmful when connected levels of information manipulation appear. Multiple departments or groups are involved, but most adversaries are in China or other countries. Propaganda departments and trolls can collaborate with connected channels, doing harm to Taiwanese society in seconds. Although the little pinks themselves are not powerful enough, they can be further utilized by the CCP. For example, back in 2000, the CCP published a white paper titled "China's PLA Prepares for Network Warfare" that highlights the multidimensional intrusion, invasion, and scams upheld mostly by trolls and bots. Within this framework, trolls and bots can first originate as volunteers in China but can be later utilized by the CCP. Therefore, to understand the relationship between the Propaganda Department and trolls, several "top accounts" from Weibo and WeChat, as well as the channels on YouTube, are key factors to examine that connect relevant ideologies from the top down. Within this connected-level structure of information operations, one should not differentiate between the government and trolls since attacks are often integrated as a whole.

2. Indirect Investment: Money Flow

In addition to contributing to direct information operations, indirect investments to the disinformation market that eschew attribution also play a significant role in the field. The MSS or the UFWD can directly donate to or sponsor certain groups that are capable of creating and spreading disinformation. For example, a local newspaper that has been circulated for free in Taiwan has been proven to have connections to the UFWD. This type of investment is covert and indirect, and without proper investigation, influence is hard to discern. Three types of indirect investment have been discovered in the case of Taiwan.

(1) Investment in the Taiwanese marketing industry: this type of investment is straightforward. Since political marketing and public relations are flourishing industries in Taiwan, it takes less effort for China to invest in certain industries than to create disinformation itself. With money provided by religious groups, gangsters, and businessmen, companies in Taiwan may take direct orders and start their own disinformation campaigns aligned with Chinese interests. These campaigns are often project-based, and companies justify their work through the statement of "it is just business." The Taiwan Affairs Office (which sets the key theme) and PLA (a money laundering organization) are key players here.

(2) Investment to create economic pressure: Sometimes, the Chinese government approaches Taiwanese local citizen to provide interests, but it seldom asks them to spread disinformation. However, these people can later be utilized to spread rumors either online or offline. For example, the gaming industry and livestream industry are often invested in by China, and livestreamers sometimes spread disinformation if necessary. They can be the nodes, but usually they are not. In crucial times, they would be coerced into spreading disinformation. Other nodes include local chiefs in Taiwan who organize paid trips to China, Taiwanese singers and actors who do their business in China and are later forced to support the Hong Kong police, and professors who visit China often to sell their books or patents there. Economic interests and reputation are often controlled by China, which creates pressure for people to "speak out" for China.

(3) Donations to entice citizens to join the network: the last kind of indirect investment is how China tries to establish the disinformation market. This includes content farms that attract rent-seekers. After content farms or YouTube channels are created, it is possible that China does not distribute articles or videos itself. Instead, China tries to pay FanPages or private Facebook groups to spread articles, paying them in foreign currency (as distributors). In one of the groups this author joined in 2019, people can make 1,500 USD per month simply by disseminating pro-China articles in Taiwan. Also, China can actually donate to someone who spreads pro-China or anti-U.S. messages (as creators). For example, in 2019, among the top 10 YouTubers who received donations online in Taiwan, seven spread pro-China messages. Actually, the top YouTuber only got 70,000 subscribers but attracted 1 million NT dollars per year. For some local channels in Taiwan, there are sudden increases in the

Chinese audience that leaves simplified Chinese comments during the pandemic, which means that influencers are vulnerable to attractions that contribute to a pro-China attitude.

Figure 6. Livestremers/Influencers Spreading Identical Messages Within One Day

Source: The author collected from Facebook and Instagram.

The second “I” (investment) does not mean that there is no money involved in the first “I”. The main difference between the two is that there is a decoupling process occurring between creation and distribution. In the first “I”, the actors might receive their own salary from the government, and the creator and distributors are all Chinese or Chinese diaspora. In the second “I”, the adversary tries to authorize Taiwanese agents to entice local citizens who want to make a profit using this framework. People who spread disinformation within this framework join the game because of economic interests, not because of their job duties. Compared with direct information operations, the Chinese government has less control with the second “I”. However, economic interests still alter behavior and contribute to existing disinformation campaigns. Outsourcing from the Chinese government generally creates a fertile environment for disinformation, which contributes to the third “I”: ideology-driven information.

3. Ideology-Driven: Human Flow

Investment may not be necessary if the target group is already pro-China. Thus, in the last kind of information operation approach, China can simply establish the "ideology market", which attracts certain groups of people who may have an incentive to criticize the government. For example, the P2P chat group could be operated by UFWD workers, and UFWD often shares videos or photos that can be manipulated within the group. In this way, information can be manipulated by volunteers in this group, who agree with anti-government messages and then further spread disinformation in an organic way.

In the discussion of Russian information operations, researchers often say that it is social media that has been weaponized. However, in the case of China, the citizens are being weaponized. These weaponized citizens voluntarily disseminate pro-China and anti-democracy messages, even preaching hatred and promoting unification between China and Taiwan. In one of the cases "I" investigated, a retired official in Taiwan joined a chat group that is related to UFWD, gradually becoming radical and cynical. He eventually shared a video with false descriptions, which other members then shared. Another example involves one of the support groups on Facebook for pro-China candidates during the 2020 election, which was actually administrated by a member of the CPPCC. Within this UFWD network, expanded by local CPPCC, Taiwanese citizens can be easily approached, joining a disinformation campaign of their own free will. Several pro-China parties in Taiwan have also established their own content farms, copying articles from Chinese state media, Weibo, or WeChat and reproducing the Chinese agenda in an organic way.

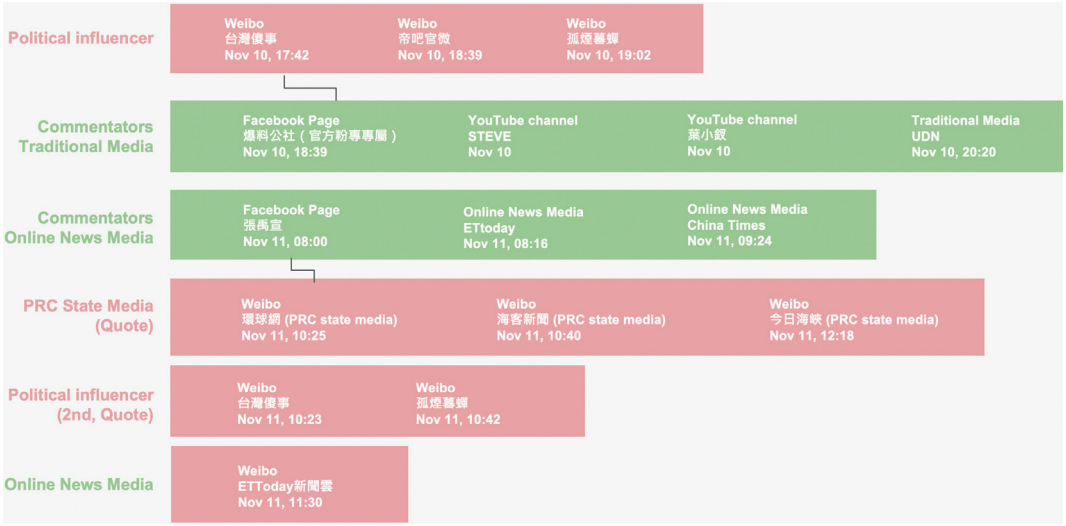

Figure 7. Sample of Dissemination Flow

Source: compiled by the author

IV. Does it Work?

The 3Is have to collaborate with each other in order to produce a measurable impact. Online and offline disinformation efforts also need to speak to each other. For example, in 2018, offline information was perfectly aligned with online propaganda. The local chief spread disinformation first, talking about how Taiwanese people could make money if Taiwan signed a peace agreement with China, and later, in the digital world—with content farm articles and YouTube channels—confirming this offline rumor. In this sense, the local chief has been incentivized by China since 2016, asking Taiwanese citizens to come to China for a paid trip; the propaganda department or the PLA manipulated this piece of information later and spread it within the digital world, the UFWD or Communist Youth League amplifying it on social media. In the end, the volunteers in the last "I" further amplified the spread of disinformation.

In 2019, the flow of money stopped due to an in-depth investigation into money laundering and tensions between Taiwan and China, which made the second "I" (investment) much harder to accomplish. Thus, China could only utilize the donation approach (which cannot be effective alone) to spread disinformation—for example, asking livestreamers to spread disinformation. In 2019, China also found a way to do this by providing profits to YouTubers, but China failed to join online disinformation

with offline efforts since the pandemic made the UFWD network hard to operate. Public awareness also increased since then, and people tended to question the information received, which created obstacles for Chinese influence operation. Furthermore, tensions within China also make disinformation campaigns inconsistent. For example, the Propaganda Department often does not align with statements by the Communist Youth League, and state media also contradicts itself due to factional struggles.

In sum, the first "I" has never stopped being influential, and it is seldom affected by the surrounding environment. The second "I"'s effectiveness is conditional, and the most effective approach currently is the donation avenue. The third "I" may not be affected by *milieu*, like the first one, but physical activities are still necessary to make sure morale remains intact. Although China has intensified its form of information warfare, the conditions in Taiwan make attacks less influential, and the Taiwanese government has established several working groups that can swiftly debunk fake news.

However, the pandemic has already shifted our way of living. We rely on Internet messages more often than before, which means offline efforts might be less useful and that online disinformation plays a much more significant role now. For example, according to a study by Doublethink, youngsters aged 20-29 are the most vulnerable group among all age groups in Taiwan in terms of believing Chinese-made disinformation;[4] this age bracket has become skeptical toward the U.S. and Japan (the two countries that China loves to denounce). The Internet has become the main channel for them to consume information, so more youngsters are now using Tiktok, Weibo, and WeChat.[5] With this in mind, the disadvantage of the investment approach may not be the main issue now, and current Chinese information operations themselves can be effective.

An attack on Taiwan-made vaccines in 2021 seems to have been successful. During the outbreak of COVID-19 cases in May 2021, the Taiwan Affairs Office (the first "I") stated that Taiwan lacked vaccines, and local chat groups with volunteers (the third "I") spread multiple messages stating that the Taiwanese government was telling lies; little pinks also flooded Facebook with fake news saying that thousands of people had died. Several YouTube channels then started to claim that Taiwan was going into lockdown; those efforts sought to create panic among the Taiwanese and

4. Po-Yu Tseng & Yun-Ju Chen, "An analysis on the impact of false information on Taiwanese

further propagated the fake patient zero footprint. A Chinese diaspora-related content farm (the first "I") joined the scheme within a week, denouncing all Taiwanese government attempts to purchase vaccines; content farms uploaded videos at the same time. FanPages and Facebook groups (previously animal-lover FanPages and DPP support groups) created by Chinese administrators (the first "I") started to attack the DPP, and fake local news websites also appeared in June. Later on, some actors and singers who have business in China (the second "I") started to mention Chinese vaccines on Weibo, implying that China could be a great help in this regard. In 480,000 traditional Chinese posts I collected on public Facebook groups and FanPages using vaccine as a keyword, 30% were conspiracy theories that denounced the vaccine—with the exception of China-made vaccines. Lastly, a local newspaper circulated for free in Taiwan, which ceased its operations in February, suddenly started to spread disinformation in print (the third "I"). The owner of the newspaper, unsurprisingly, is connected with the UFWD network. In the end, although the investment approach is not typical in this case, the attack was still successful, creating distrust within Taiwanese society.

Using the 3Is framework to assess and evaluate Chinese information operations can be useful. However, since Chinese strategies evolve, this model is certainly not comprehensive. That being said, taking the Taiwanese experience as an example, the world should understand how harmful Chinese-style information operations can be, and a strategy for countering them should soon be established.

---

voters," *Doublethink Lab Medium*, May 6, 2021, <https://medium.com/doublethinklab/an-analysis-on-the-impact-of-false-information-on-taiwanese-voters-c061500a898c>.

5.〈抖音、小紅書魅力在哪？新世代熱門 APP 大揭密，Z 世代說給你聽〉, *Readr*, June 27, 2021, <https://www.readr.tw/post/2572>.