China's Cognitive Warfare Against Taiwan and Taiwan's Countermeasures

Ying-Yu Lin

Assistant Professor
Graduate Institute of International Affairs and Strategic Studies,
Tamkang University

Abstract

As early as December 2003, China, based on lessons learned from the Iraq War earlier that year, formally launched the concept of public opinion warfare, psychological warfare, and legal warfare. In 2014, the People's Liberation Army (PLA) went one step further and came up with the concept of "mind superiority," a Chinese term which means literally "brain control power." It was set to be used in operations against Taiwan. The most recent digital public opinion warfare tactics against Taiwan, combining disinformation with applications of information technology, are concrete examples of this concept being put into practice. This paper discusses the subject from the perspective of cognitive warfare as it is commonly known. It includes an analysis of relevant cases to identify the PLA's new moves and its customary tactics, and seeks to provide a reference for Taiwan in the development of countermeasures against the PLA.

Keywords: Disinformation, Cognitive Warfare, China Three Warfare, Fake News, Taiwan Security

I. Introduction

Since its establishment in 1949, Communist China has never relinquished the option of using force against Taiwan. In addition to traditional military means, the People's Republic of China (PRC) has also used the practice of creating propaganda and lies to undercut Taiwan's national security. Such tactics are not new to the Republic of China (ROC) government; Chinese communists used propaganda to shape

public opinion to their advantage during the Chinese Civil War, which resulted in the nationalist-led ROC government's retreat to Taiwan in 1949. Now, with rapid progress in technology, the general public has become increasingly dependent on information technology. This has brought a new twist to old-style propaganda methods, contributing to the formation of a type of digital technology-assisted digital public opinion warfare between the two sides of the Taiwan Strait. Disinformation and "fake news" are the techniques most commonly used in warfare of this kind.[1] They became even more specialized after 2016. This development may have something to do with the People's Liberation Army's most recent military reforms, launched in 2016, and the accompanying establishment of the Strategic Support Force (SSF). The resultant combination of public opinion, propaganda, and information technology allows traditional propaganda methods to reach target audiences within a short timeframe with the assistance of technology. With the help of big data analysis, actors can have a good grasp of the geographical locations and political affiliations of large numbers of people and thus be able to target specific groups of people precisely.[2]

Such campaigns are quite different from devastating traditional military operations, but they can still achieve certain effects on the internal politics of a targeted country. These can be used for greater leverage in world politics. The methods for achieving these effects not only cleverly go around the traditional definitions of armed conflict or war, but also cause damage to more nations than the target one. Even if victimized countries take steps to clarify disinformation or find out the truth behind disinformation campaigns, there is always a way to change tactics by using derivatives of the original methods, partly because of a lack of clear legal definitions for the actions involved and partly because of the protections under

---

1. Due to the fact that the term "fake news" includes misinformation intentionally spread by certain people or false press reports, it is prone to misinterpretation. Therefore, some academic institutions and the government sector have started to use "disinformation" instead. For the convenience of the reader and to avoid misunderstanding, this paper uses "disinformation" as referring to "news information that has been doctored and spread through media outlets."

2. John Costello & Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (DC: National Defense University Press, 2018). pp. 1-68.

Figure 1. China's Cyber Army

Source: Depositphotos.

"freedom of the press." As Sun Tzu says in *The Art of War*, "The supreme art of war is to subdue the enemy without fighting." So, how to use propaganda methods to weaken the enemy nation's strength before the start of military action, in hopes of inciting internal conflicts in that nation and fueling public distrust of government authorities at the same time is likely to become an option for communist China. It poses a challenge to all democracies.[3]

---

3. P.W. Singer & Emerson T. Brooking, 《讚爭：「按讚」已成為武器，中國、俄羅斯、川普、恐怖組織、帶風向者、內容農場，如何操縱社群媒體，甚至⋯⋯不知不覺統治了你》 (*LikeWar: The Weaponization of Social Media*), trans., Lin Shu-ling (Taipei: Willful Publication Company, 2019), pp. 241-250.

That public opinion campaigns over the Internet exert influence on the general public is nothing new. Formerly, in the field of business marketing, certain organizations would hire online public relations companies to post product- or issue-specific messages on the Internet or respond to website visitors' messages on behalf of the clients in a way that served to make the clients known to more people. People doing these jobs are called "review spammers." In communication studies, there is the spiral of silence theory. According to this theory, review spammers can be made to look like opinion leaders, capable of "leading the wind," as is commonly called over the Internet. Internet-based social media platforms usually allow members to post messages with specific intentions, which receive positive responses from those in agreement. People who disagree with these posts keep silent most of the time. Some readers may choose to share the posts, but they do it only after a selection process based on the position they take. This leads social media platform members to become more assertive about their views, forming a condition where "people who follow different paths cannot plan together." These people thus become "filter bubbles."[4] People trapped in filter bubbles (since they do not have different opinions as a reference) tend to become biased toward certain issues. They cannot accept things as they are. They are thus prone to be used by people with ulterior motives to send disinformation or negative content to certain groups of people in an attempt to incite them to do something or make remarks within expectations. It is just one possible way of using them.

Additionally, many online topical forums, despite their efforts to encourage diversified points of view, normally end up being flooded by shallow comments or emotional criticism without being able to provide a chance for reasonable dialogue or discussions. This results in a win by the side with superiority in numbers, which is just what review spammers want. People trapped in filter bubbles have been developed by communist China into the so-called "50-cent party." Members of the party make comments on political or military issues. They normally get paid for each reply to an

---

4. Wang Chih-chien & Chen Tsai, 《假新聞：來源、樣態與因應策略》(*Fake News: Sources, Patterns and Countermeasures*) (Taipei: Future Career Publishing Corpora-tion, 2019), p. 108.

Figure 2. Internet Flooded by Shallow Comments or Emotional Criticism

Source: Depositphotos.

online message. Even if social media platforms try to block or ban accounts suspected of belonging to 50-cent party members by activating a system evaluation mechanism, the account holders can still get around those via virtual private networks (VPNs) or buy fake accounts in large numbers. They can even use Botnet-controlled response systems.

II. 50-Cent Party's Transformation and Newest Developments

Notably, review spammers are undergoing a transformation. They no longer wait for clients' requests or focus their efforts just on making comments in favor of specific products or messages. They take the initiative to make an issue of certain political developments. They even use negative propaganda campaigns to shape a situation to their advantage. They may also choose to play a double game with two opposing camps by pretending to be members of either camp and posting messages that provoke or displease the other side. They leave noticeable clues on purpose for either camp to track down sources of the messages. They aim to exacerbate the confrontation

between the two sides and weaken either side's unity. Cyber forces of this type usually aim to capitalize on the issues on the public agenda. They also take advantage of the high interactivity and real-time information and response characteristics of social media platforms, ranging from the earlier bulletin board system (BBS) that allowed instantaneous message-posting and response to current social media platforms that use share and like functions to encourage posters and boost people's political participation.

The actions discussed above are not what the old-school 50-cent party was capable of. In place of the 50-cent party, there are now specialized groups that are well aware of public sentiment, social developments, and the distribution of preferences by group. They have enough skills and knowledge to successfully attain the goal of affecting public sentiment. This provides a new direction for the "three warfares" in the digital age. In terms of the concept of mind superiority or brain control power, the PLA stipulated in 2014, in addition to the efforts to control the air, sea, land, and Internet, the struggle to control the brain through the combined use of the media and propaganda will be a major battlespace in future, a hotly contested realm for sure.[5] Taking an advantageous position in this new realm necessitates technological assistance. Cyber forces will not focus their efforts only on stealing intelligence and preying on system vulnerabilities. They also have to launch new forms of technology-assisted public opinion warfare to meet the requirements of war in a new era.[6]

Threats posed by the PRC's cyber forces have been repeatedly mentioned in reports by major information security companies and several governments. The reports have called attention to the fact that China's cyber forces have greatly improved their combat capabilities following recent military reform. However, the

---

5. Regarding mind superiority, please check this source: Zeng Huafeng & Shi Haiming, 《制腦權：全球媒體時代的戰爭法則與國家安全戰略》 (*Mind Superiority: Rules of Engagement in Global Media Age and National Security Strategy*)(Beijing: PLA Press, 2014), pp. 180-196.

6. Lan Zhouda & Ma Chienguang, 〈制腦權視野下的新型網路戰─以顏色革命為例〉(New Types of Cyber Warfare in Light of Competition for Mind Superiority: Color Revolution as an Illustration), *National Defense Technology*, Vol. 36, No. 6, December 2015, pp. 57-62.

Figure 3. Cyber Space Is a New Battlefield

Source: Depositphotos.

key to the improved combat strength is not enhancement in technical capabilities but overall performance following structural integration. Information security company reports show that between 2015 and 2018, China's cyber forces were generally in an inactive state or showed no signs of action at all. However, starting from the second half of 2018, these units resumed their cyber warfare campaigns, showing some differences in the tools, methods, and targets selected.[7] This is ostensibly related to the SSF's internal reorganization and mission reassignment. After all, cyber warfare is not bound by limits set by geopolitical strategy. Moreover, apps developed in China or mobile phones made there have managed to gain access to global markets because

---

7. Wu Chi-hsun, 〈中國網軍重現江湖，8個駭客組織回歸運作〉(China's Cyber Forces Back Online: Eight Hacker Groups Resume Operation), *IThome*, October 5, 2018, <https://www.ithome.com.tw/news/126295>.

of their low prices. These devices are used to collect users' personal data, which may not necessarily be a direct threat to users. The collected information, however, may become research materials for China in its planning of future disinformation campaigns.

From the discussion above, we can ascertain the steps that China will take to launch disinformation campaigns. It is a completely new battlespace, an additional battlespace on top of those for the control of the sea, air, and electromagnetic spectrum.

III. China's Disinformation Campaign Tactics

China's cyber forces use the following methods to spread disinformation:

Using topical issues: Social issues that can easily create confrontation between groups with opposing views are utilized to widen division in targeted societies. They have been used to spark debates and confrontations over the new "one fixed and one flexible day off per week" working hours scheme launched by the Tsai administration, homosexual rights (legalization of same-sex marriage), pension reform, and labor strikes. Sensational and hate-provoking headlines were selected by certain groups in their coverage of those confrontations in an attempt to increase divisions within the opposing camps and widen divisions in society.

A case study: In April 2017, groups that opposed the Tsai administration's proposed pension reform posted to Facebook groups messages entitled "Civil Servants Treated Not as Well as Vagabonds." The messages went like this: The Taipei City Government provides a low-income subsidy of NT$18,000 per month to each homeless person around Longshan Temple, an amount which was raised to NT$30,000 for a homeless person with a spouse. The posters of the messages complained that despite having worked hard for many years to reach their current positions, military personnel and civil servants were now being treated worse than homeless people. This was meant to incite the Taiwanese people and foster antagonism, and thereby undermine social harmony. The incident greatly disturbed the Taipei City

Figure 4. The CCP Aims to Exacerbate Divisions in Taiwan

Source: Depositphotos.

Government, which issued a special press release to provide clarifications.[8]

Public opinion campaigns: Botnet-controlled accounts are used to flood social media message boards. They leave messages on Facebook, Instagram, the PTT Board, YouTube and other main websites to "lead the wind" (or guide public opinion) or criticize dissidents who are deemed to be not one of them. In addition to large amounts of messages serving to "lead the wind," verbal bullying is also employed to silence people.

---

8. Chang Kai-hsiang,〈遊民每月爽領 31000 ？北市府：根本沒補助〉(Rumor Buster: Taipei City Government Denies Giving Each Vagabond NT$31,000 per Month), *Liberty Times*, April 11, 2017, <http://news.ltn.com.tw/news/politics/paper/1093179>.

Processing news texts for recirculation: News stories are "processed for recirculation back in Taiwan." China's content farms process Taiwan news stories in a way that turns them into half-false and half-true fake issues. These processed news stories are then sent back to Taiwan for large-scale recirculation and to sow confusion.

Intentional spread of mis/disinformation for specific purposes: Disinformation disguised as tips for dummies with "elder pictures" as cover images is spread from one Line group to another for the purpose of propagating lies (Line is a communication app highly popular in Taiwan). On this platform, a mere share button will make a message become viral and eventually hard to control.

Selective juxtaposition of images and content unrelated to each other to convey certain messages: Methods like telling a story by looking at a picture, but only told in a twisted manner that leads to a mismatch between an image and the time and location of the event depicted in the image, are used to incite political groups to confront each other.

IV. Possible Countermeasures

Democracy and freedom are Taiwan's core values. Nevertheless, Taiwan's main adversary is now trying to subvert and divide the Taiwanese government by taking advantage of the democratic system and freedoms cherished by the Taiwanese. This does not mean that Taiwan needs to go back to the old days when the government adopted authoritarian methods to keep tabs on the population. This would constitute a democratic regression. Moreover, tight monitoring of the public would only result in more crimes and rebellions. China's Internet real-name registration system and *Internet Security Law*, for example, are intended to fight false statements online and cyber crimes. However, as the saying goes, "Evil always outdoes good." Stringent Internet controls could only give an impetus to cyber crimes (like stealing and selling accounts) and anonymous communication. As a government tightens its Internet controls, it runs the risk of fostering more cyber crimes.

In view of the overall situation, Taiwan should make greater efforts to ensure that public opinion goes in the right direction, providing verified information, and

Figure 5. President Tsai Ing-wen Attends Taiwan CYBERSEC 2021

Source: Photo by the author.

establishing rumor-debunking channels to reduce the possibility of disinformation spreading. The government should also make public on a regular basis its administrative performance and relevant information; it should even take the initiative by releasing rumor-debunking "tips for dummies" while securing its communication channels both within and with the outside world so as to take the lead on information management. Relevant government agencies should have their spokespersons develop public relations crisis management capabilities and establish links with traditional and social media in order to issue timely clarifications when disinformation is about to spread and to prevent against the kind of information manipulation that can spark internal unrest. A third-party fact-checking mechanism could also be established in cooperation with the civilian sector to bolster credibility.[9]

---

9. Wang Chih-chien & Chen Tsai, 《假新聞：來源、樣態與因應策略》(*Fake News: Sources, Patterns and Countermeasures*), pp. 157-171.

The U.S. has also begun to consider amending relevant laws to be better able to cope with disinformation, including the possibility of listing the U.S. branch office of *Xinhua News Agency* as a public relations company, rather than a media organization. The U.S. has realized that China is taking advantage of the U.S.' insistence on maintaining freedom of the press and democratic values (freedom of the press as specified in the amendments to the U.S. Constitution and cited by U.S. judges in court on multiple occasions) to develop its "sharp power."[10] Even if *Xinhua* were no longer listed as a media organization in the U.S., its reporters would still get press passes. However, public relations companies in the U.S. have to make public information about how they operate. The U.S. expects the move to curb media offensives launched by China. Although there were many precedents of U.S. legislating restrictive acts against certain specific hostile countries, those laws were mostly made in the 1970s, some even dating back to the 1950s. Of course, the restrictions set at that time could not cover information technology and relevant equipment. As such, most of the laws and regulations have to be amended to keep up with the times. It also suggests that the U.S., after a long-term miscalculation of threats posed by China, has started to recognize what Beijing has achieved with the three warfares. The U.S. has sought to do the same to China by resuming studies on the three warfares and conducting interdisciplinary studies and integration that cover intelligence, communication, and public relations studies. The possibility of "countering the three warfares with the three warfares themselves" is being discussed. Possible countermeasures are as follows:

1. A High-Low Mix of Mainstream Media and Sub-Media

China often relies on a high-low mix of *Global Times* and the *People's Daily* in its choice of a mouthpiece for its official stance on specific issues. The *People's Daily* is a media organization owned and run by the CCP, more authoritative in terms of the opinions it expresses on behalf of the Party. The *Global Times*, though also categorized as state-run media, is often more like an instrument to gauge where

---

10. Regarding expansion of communist China's media, please check this source: He Qing-lian,《紅色滲透：中國媒體全球擴張的真相》(*Red Infiltration: The Reality of China's Global Media Expansion*) (Taipei: Gusa Publishing Company, 2019), pp. 197-223.

the wind blows or serves as an outlet for hawkish members of the Party. It is not as authoritative as the *People's Daily*, and tends to be functional most of the time. Although Taiwan also owns media organizations that are owned by the government or whose editorial line tends to reflect the government's, they nevertheless have local audiences as their main market. It may be feasible to have newspaper columns devoted to the issue or establish new media outlets specifically for the purpose. There is no need to get these ideas into print. In the digital age, Internet-based media outlets can achieve similar effects. They may even create, alongside state-run media, an offensive capability that features an "alternation between regular and irregular means and a combination of real and fake moves." Sometimes, propaganda campaigns of a particular sort or active moves in a certain direction are not necessarily suitable for implementation by state-run media.
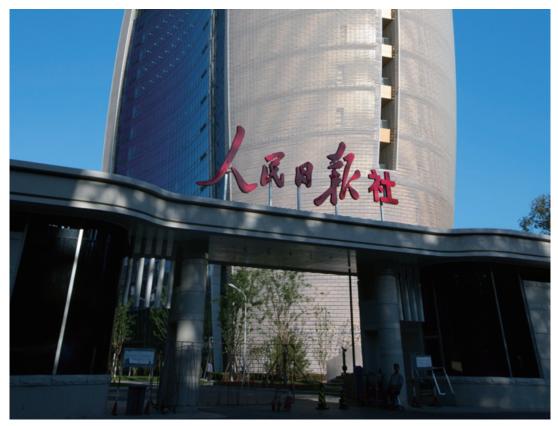

Figure 6. People's Daily Headquarters

Source: Morio, "People's Daily Headquarters," September 2, 2015, *Wikipedia*, <https://zh.wikipedia.org/zh-tw/File:People%27s_Daily_Headquarters_2015_September.jpg>.

2. Trans-Departmental Rapid Response Task Force

Given that disinformation comes in different forms, touches on a great variety of issues and that there is even "composite disinformation," the content of which may have to be jointly handled by multiple government agencies, there is, therefore, the need to form a trans-departmental task force (or office) in response. What should be avoided is a hasty response made for the sake of expedience or getting the job done as soon as possible. It will only be seized by the opponent as an opportunity to make a big fuss and thus undermine its legitimacy. Therefore, it is necessary to establish a trans-departmental task force in advance and to set up relevant research institutes (preferably private think tanks with no official ties to the government or journalists) to form a "red army" that plays the role of the imaginary enemy competing with the task force in realistic scenarios. The task force will undergo tests in different scenarios, and the government's standard operation procedure (SOP) for the handling of disinformation is also to be consolidated to be able to respond quickly to emergency situations. All these measures are meant to achieve timeliness. If disinformation cannot be contained within the shortest time possible or the government fails to make a clarification or explanation within 24 hours, there is a great probability that the disinformation will start to exert influence on the general public. By the time people buy it, explanations and corrections will be useless.

3. Using Artificial Intelligence Technology

Anti-disinformation efforts are an arduous job without corresponding rewards. After all, the enemy always lurks in the shadows, while we in democracies are exposed to light. Creating disinformation costs much less and takes much less time than fact-checking efforts. There is just not enough manpower to cope with disinformation in all its forms. However, with the assistance of technology, we can effectively detect some types of disinformation early on. Locating IP addresses, for example, is a basic way to identify a source of disinformation. Some participants in an online discussion about an event or earlier posts that sparked the discussion might not have any relevance to the place where the event occurred. For example, many online posts discussing Taiwan politics or related issues have been found to come from African countries. Some of these posts contain texts that used a lot of Chinese

expressions or phrases not commonly seen in Taiwan. It shows that the posters might have some ulterior motives for writing the articles. Artificial intelligence technology can be used to make a preliminary analysis of online posts, and machine learning used in the process can automatically screen out some potential problems, reducing the workload for humans.[11]

4. Leveraging All Available Resources to Achieve Comprehensive Defense

For Taiwan's Ministry of National Defense (MND) and other government

Figure 7. Application of AI Technology

Source: Depositphotos.

---

11. This part of discussion is based on an interview with famous hacker Clarence Chio in April 2018. Regarding studies on AI, please check his book: Clarence Chio & David Freeman, *Machine Learning and Security: Protecting Systems with Data and Algorithms* (CA: O'Reilly Media, 2019), pp. 275-324.

agencies, a crisis also means a possible turn for the better. Public opinion warfare campaigns launched by China against Taiwan provide a perfect opportunity for us to bring our psychological warfare capabilities into play and to make preparations for a comprehensive defense for all sectors of society. Military-themed TV drama series produced by the Taiwanese military as part of political education for service members, or traditional media programs, have limited effectiveness against disinformation. However, as the PLA keeps flooding Taiwan with increasing amounts of information, MND spokespersons and private media can join hands to release verified information at appropriate moments. This will not only neutralize disinformation campaigns launched by China, but also provide a chance for the general public to understand how much work service members have done and the great their contribution they have made to the country. The military-owned *Youth Daily* and weekly political education TV programs for service members may have a column or segment for either military or civilian specialists in the field, who can use their expertise to point out false information PLA-affiliated media outlets mention when talking about defense issues. They may also identify through these random pieces of information what kinds of threats the PLA can pose to Taiwan. It is a good opportunity for the Taiwanese people to discover how they can prepare themselves psychologically against dangers in times of relative peace.

The PLA's "far-sea long voyage" missions provide a salient example of what can be done. Prior to the missions, the PLA contacted media organizations to produce mini-movies for its flight missions or offer other assistance such as doctoring the photo of a bomber against the background of mountain ranges in the distance. The photo, once made public online, instantly prompted media of the two sides of the Taiwan Strait to make extensive coverage. Some people identified a mountain peak in the photo as Taiwan's Yushan. However, a follow-on analysis of the photo showed that judging from the angle from which the photo was taken, the mountain was not Yushan. Specialists with flying experience also pointed out other problems with the photo. Taiwan's MND can form a rapid response team to deal with disinformation and need not necessarily have to hold a press conference using the Military Spokesman's Office. A forum can be held instead, attended by journalists from military media organizations and Internet-based news websites, as well as academics familiar with defense affairs. They can debunk China's disinformation right away. This is a feasible option. We

can also produce mini-movies to highlight the hard work that the ROC Air Force has made in air defense, interception of intruding planes, and scrambling of planes for emergency situations. Such films would help the general public realize that military training is not making a lot of noise for nothing and that the PLA's threat to Taiwan is real. This is an example of a comprehensive defense at its best.

V. Conclusion

In 1999, an influential book titled Unrestricted Warfare was published in China.[12] Now, with the assistance of digital technology, the unrestricted warfare

Figure 8. A PLA Air Force Xian H-6 Bomber and Mountain Range in the Background

Source: Huang Yi-yuan,〈中共轟炸機俯視玉山？國防部籲勿以訛傳訛〉(CCP Bombers Overlooking Yushan? The Ministry of National Defense Urges not to Spread Lies!), *CTS*, December 17, 2016, <https://news.cts.com.tw/cts/politics/201612/201612171832328. html>.

---

12. Qiao Liang & Wang Xiangsui,《超限戰》(*Unrestricted Warfare*)(Beijing: PLA Art and Literature Publishing House, 1999), pp. 165-184.

adopted by China has adopted new variations. It has been combined with the concept of "three warfares" proposed in 2003 to form an intensified struggle to achieve mind superiority. In view of the fact that most countries now follow the principle of "fighting without breaking" in their engagement with each other, governments have generally become more cautious in their use of force. Spreading propaganda through the media is now the norm, and consequently, the media have become the main battlespace between countries. Due to the popularization of Internet technology, digital technology-assisted public opinion warfare via the Internet will be increasingly an area of focus for countries. It is a completely new area, one in which nations will actively develop their capabilities. How to be one move ahead of the enemy, take precautionary measures, and take the initiative to control commanding heights in digital public opinion warfare is also a subject for Taiwan to explore and discuss in the years to come. Taiwan has an unequaled body of knowledge about China and the PLA. However, in addition to its advantage in academic research in the field, Taiwan should also consider the possibility of turning this knowledge into an invisible form of weaponry, which requires maximization of information superiority and analysis of China's internal problems. In doing so, Taiwan can not only counter the China's "three warfares," but also have the capability to strike first to gain the initiative and prevail over the enemy. By "countering the enemy's three warfares with their three warfares," Taiwan can put itself in an unconquerable position.