DisinfoLab
thedisinfolab.org

The Fake Wall of China

Deception through Hired Social Media Mercenaries

PART-1

Table of Contents:

Introduction ____ 3

Part 1: Anti-CCP Protest against Zero-Covid policy ____ 5

Section A: The Great Firewall of China Collapsing ____ 6

Media Control ____ 7

Section B: Spam Network Ops Analysis ____ 8

Part II ____ 13

"Beautiful China": a Case Study in Deception ____ 13

A Pro-China propaganda social media network ____ 15

Section A: Beautiful Propaganda ____ 15

Section B: A 'Model' spam-network ____ 18

Section C: DP borrowing network ____ 23

Section D: A dissociated communication ____ 26

Section E: A Link-sharing Kinship ____ 28

Part III: Twitter Analysis ____ 31

The Motive ____ 33

The Reply Army ____ 38

The Quote masters ____ 39

The Media abundance ____ 40

Part IV: China-Pak Propaganda ____ 41

Putting Resources to Good Use: Galwan Valley Skirmish ____ 42

20th National Congress of CCP & Propaganda follows ____ 42

Conclusion ____ 47

Introduction

Widespread protests against the Chinese Communist Party (CCP) are going on across various major cities in China for the past few months. The country's prolonged & strict lockdown rules under the CCP's zero-COVID policy have become a source of discontentment for the citizens who are locked in their homes. And the recent unfortunate fire incident in Ürümqi, Xinjiang that took many lives, triggered nationwide protests as people took to the streets to show their agony.

Upon looking for the news about the protests in China on social media, the search results did not show the actual updates. But what was found was a plethora of spam posts related to gambling, e-gaming, dating sites, and adult content.

In the wake of such developments, a network of accounts on social media was found to be lurking to suppress the sequence of events. Chinese-language accounts in large numbers were found to be covering up the anti-establishment protests in China through a massive scale of spamming operations.

Institutions and journalists have now started identifying such spam networks that operate to avert the leakage of anti-China information beyond the borders. However, it's no new phenomenon. These spam networks working for China have now been existing for years and have been under our observation.

These spam networks are a part of Chinese operations on social media. They are primarily created for polishing China's global image as according to them, the western world is denting China's image as human rights violator. Hence, their day-to-day chore is to spam social media with pictures of Chinese food and sceneries in large numbers, only to push pro-China and political posts promoting & protecting China's interests.

Another motive of this network is to grow each other in the ploy of running bigger social media campaigns in the future. These accounts seem to be working disjointly; in isolation to show that they are not connected. However, our findings showed that they have been associated with the same network and share common followers.

While the Chinese disinformation industry is mainly focused on presenting a positive image of the Middle Kingdom, they also indulge in targeting other countries when needed. The targets range from the US to India. In this endeavour, particularly against India, China finds Pakistan a willing partner.

These two nations have common interests and even have a border dispute with India. While Pakistan and India have a territorial conflict over Kashmir, the Sino-Indian territorial dispute lies in the Himalayan region. Such conflicts don't just unfold on borders with military intervention, but social media becomes a useful tool in the demonstration of disinformation propaganda. It was observed that Chinese propaganda once planted on social media was taken up by Pakistani social media over the skirmish that took place between Indian and Chinese soldiers in the Galwan Valley in 2020.

The Chinese operations on social media are never-ending and, in our effort, we have been able to dissect a few of such networks that are run for/ on behalf of China to control the narrative in the favour of China.

Part I: Anti-CCP Protest against Zero-Covid policy

As early as March-April 2020, when the deadly virus was taking a stride and suspicions about China had begun, Ops deployed pro-Chinese propaganda to manipulate its global image. The narrative was simple: to tout China as a global leader and laud its ability to surpass the western superpowers in handling the pandemic. [1] [2] [3]

Not one, but scores of articles were written in appreciation of how China was handling the COVID situation, downgrading other nations. [4] Some even stated that China has a meritocratic government and opined that the post-pandemic *"China will accelerate both for the public's benefit and the balance of strong markets and good governance will be an appealing model for other countries".* [5]

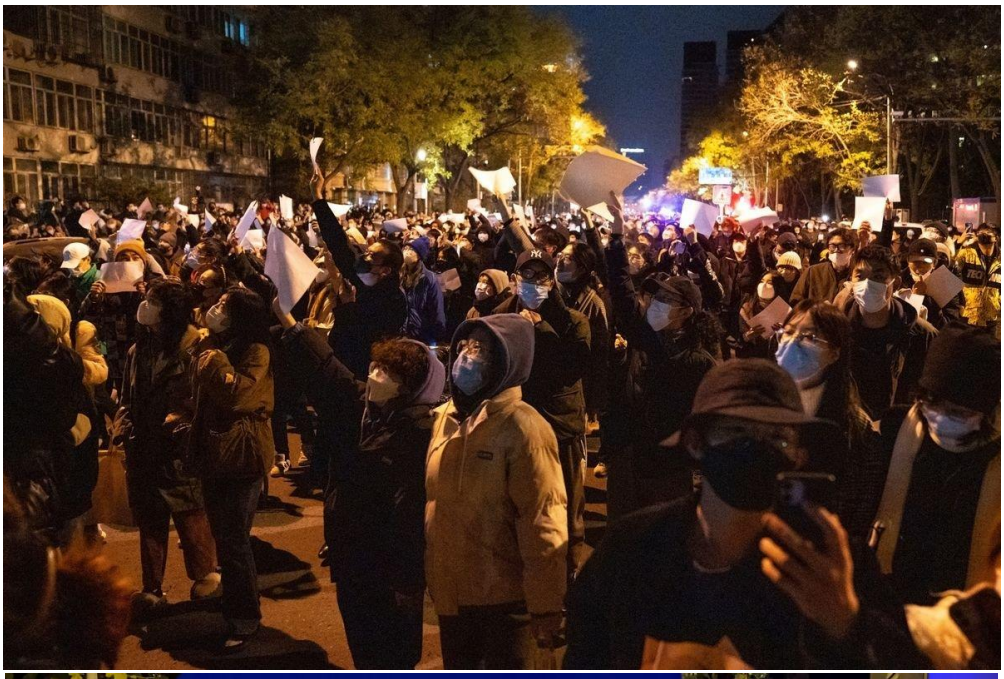
Efforts were made to promote the narrative that China would emerge as the economic leader in the aftermath of the pandemic. And that China's zero COVID policy would set an example to contain the virus.

[1] https://www.bloomberg.com/news/articles/2020-10-18/china-s-rebound-helps-to-stabilize-a-shattered-world-economy
[2] https://edition.cnn.com/2020/10/18/economy/china-q3-gdp-intl-hnk/index.html
[3] https://www.wsj.com/articles/chinas-economy-is-bouncing-backand-gaining-ground-on-the-u-s-11598280917
[4] https://www.npr.org/2020/09/01/908222940/china-india-handled-covid-19-differently-their-results-differed-too
[5] https://www.economist.com/by-invitation/2020/04/20/kishore-mahbubani-on-the-dawn-of-the-asian-century

Section A: The Great Firewall of China Collapsing

In 2022, China entered its third year of the COVID-19 pandemic despite Beijing's stringent "Zero-COVID" policy. Beijing is not only struggling to contain the virus, but its '*Great Firewall of Internet Censorship'* seems to have taken a toll. Several videos of the lockdown being imposed in various parts of China started surfacing on social media. Beijing is known to have the most sophisticated internet censorship that the People's Republic of China deploys to control or even take down internet content from within China's borders.

However, visuals that have emerged from within China about exposing the situation in the country have undermined its '*Great Firewall'.*



Most recently, videos of protests in China emerged on social media following a tragic incident in a residential high-rise building in Ürümqi, Xinjiang, China on November 24, 2022. The unfortunate incident resulted in the loss of 10 lives while over nine non-fatal injuries were reported. Subsequently, mass anti-lockdown protests swept the streets in China seeking the resignation of Xi Jinping, who took the oath as the leader of the country for his third consecutive term in October 2022. [6]

Media Control

China has the most restrictive liberty for media and has complete control of the censorship of the news and information outflow through the state-affiliated media. The state media regularly spreads the pro-CCP narrative but was nowhere in the picture in covering the news about the protests. Notably, the state-affiliated media namely Global Times, CGTN, and Xinhua among others, didn't do a single coverage of the widespread protests, which took/are taking place in major cities in China.

On the other hand, there were clampdowns on foreign journalists who were reporting on the live protests happening against the country's zero-COVID policy. BBC journalist, Ed Lawrence was beaten and arrested before getting released. While the China correspondent for Swiss broadcaster RTS, Micheal Peuker was detained by the police briefly for reporting live protests in Shanghai.

[6] https://edition.cnn.com/2022/11/26/china/china-protests-xinjiang-fire-shanghai-intl-hnk/index.html

Assuming that the West's reports and coverage of the worsening situation in China were forthcoming, the Chinese spam network started working in full swing. As soon as the news broke about the fire, a plethora of Chinese accounts began posting unrelated pictures and videos to drown the posts related to the accident in Xinjiang. The spam network accounts used 乌鲁木齐/ Ürümqi (in Chinese) in their tweets to start spamming on Twitter.

What is a Spam Network?

The whole operation carried out by the set of accounts which can be large in numbers, is often defined as a 'Spam Network'. The core objective of a spam network is to flood social media platforms with its content to take over a large chunk of cyberspace and further achieve an objective. This would enable them to appear in anyone's search results or on their timeline and successfully cater to them with their spam content flooding.

News of protests against the zero-COVID policy was pervading various parts of China for a while now. The protests were in clusters and not widespread. However, the deadly fire incident in Xinjiang brought them all together and gave impetus to wider and more coordinated nationwide protests.

Section B: Spam Network Ops Analysis

Concealing these bigger-scale anti-establishment protests asked for a much-bigger social media operations. As the protests broke out in major cities in China including Shanghai, Nanjing, and Beijing, the Spam Network was mobilized. The network here was spamming Twitter with irrelevant posts to sink the legit search results about the protests. Since protests were pervading different major cities in China, the spam network also picked the names of cities for pursuing its spam operations and covering legitimate news.

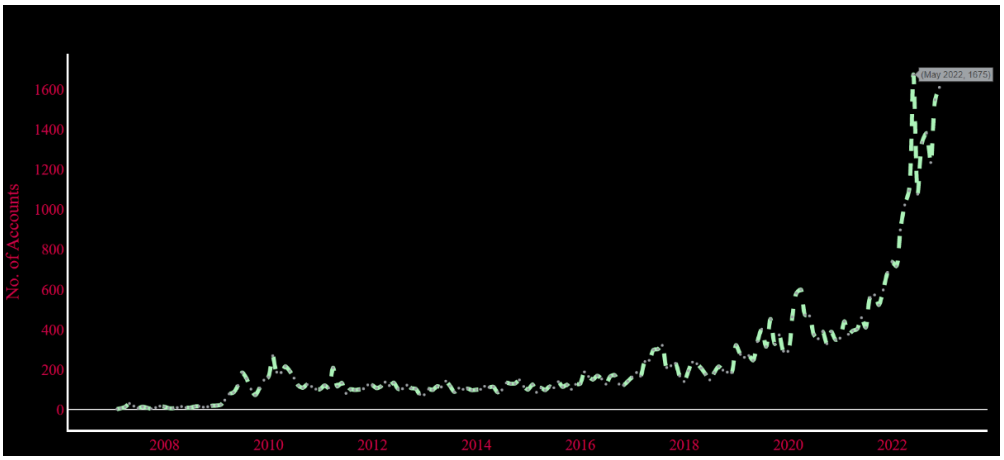
Hence, we picked the name of different cities in China including 北京 (Beijing), 上海 (Shanghai), 成都 (Chengdu), 天津 (Tianjin), 广州 (Guangzhou), 深圳 (Shenzhen), and 重庆 (Chongqing) as keywords to understand the operation of this spam network.

These accounts were spamming the platform with promotional posts of dating sites, escorts, gambling, and e-gaming all by using the names of all the major cities where protests broke out. The frequency of spamming was such that these accounts were tweeting the same content in a gap of a few seconds and minutes.

On further analysis it was found that most of these accounts were newly created this year with a followers' count below 10. So, we used 北京 (Beijing) as the only keyword for analyzing the tweets done on November 26-27, 2022, we found that the tweets were in large numbers (approx. 1,80,000 tweets) by 46,002 unique accounts.

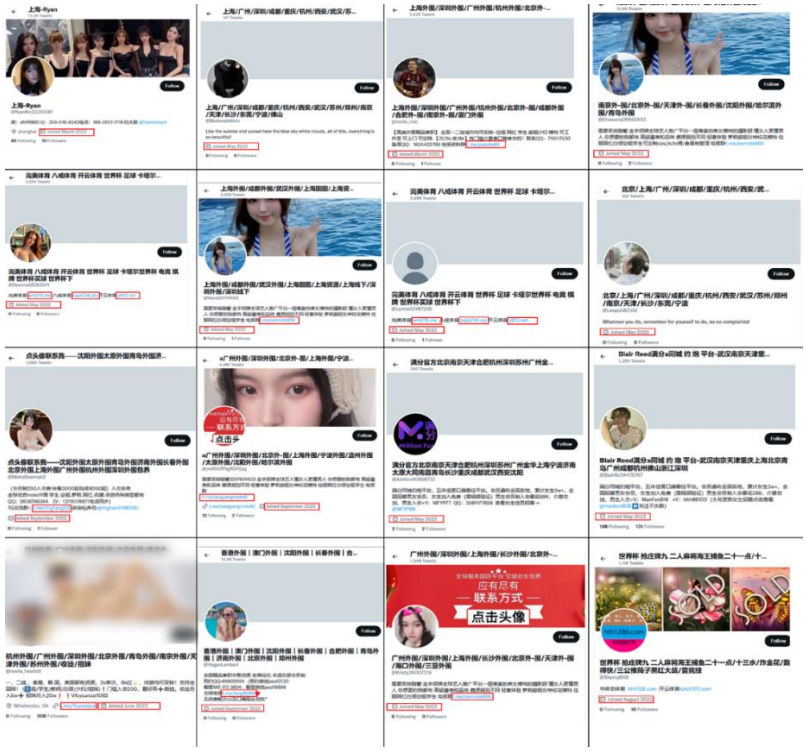
And upon analyzing those accounts that tweeted using 北京 (Beijing) keyword, we found that 9865 accounts were created since May 2022. Most numbers of accounts i.e., 1675 accounts were created in May 2022 followed by:

a. 1077 accounts were created in June 2022.
b. 1336 accounts created in July 2022
c. 1382 accounts created in August 2022
d. 1235 accounts created in September 2022
e. 1549 accounts created in October 2022
f. 1611 accounts created in November 2022

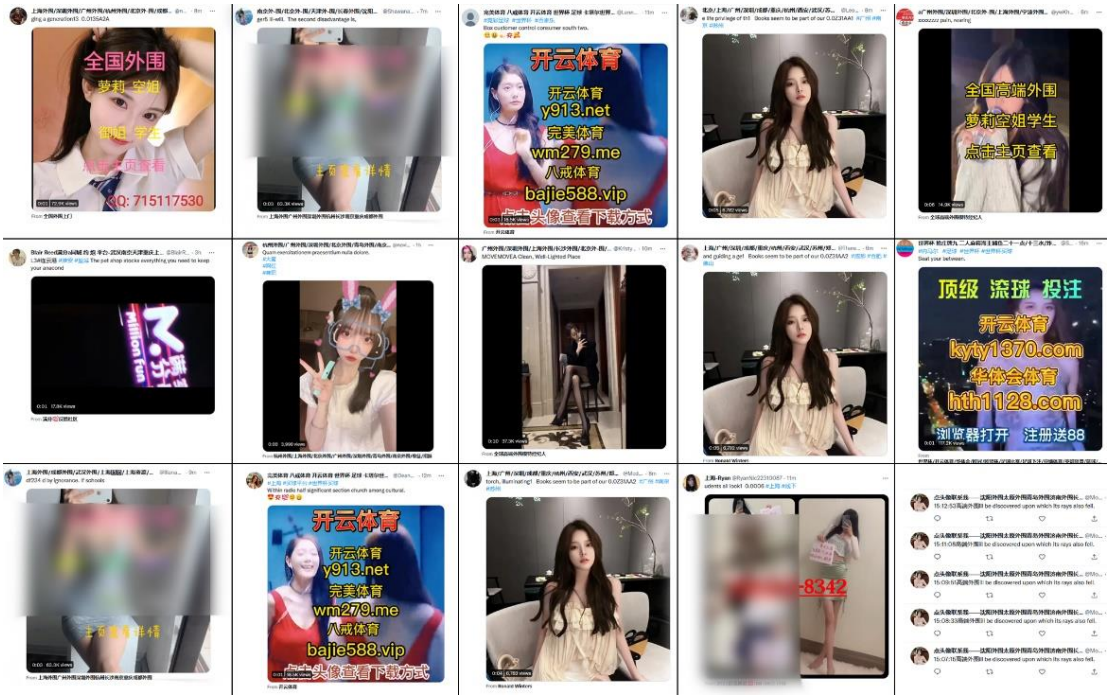


Accounts' creation timeline

The following sample shows the accounts that were created in 2022 and their screen names are in Chinese. Furthermore, all these accounts have seemingly malicious links in their bios.

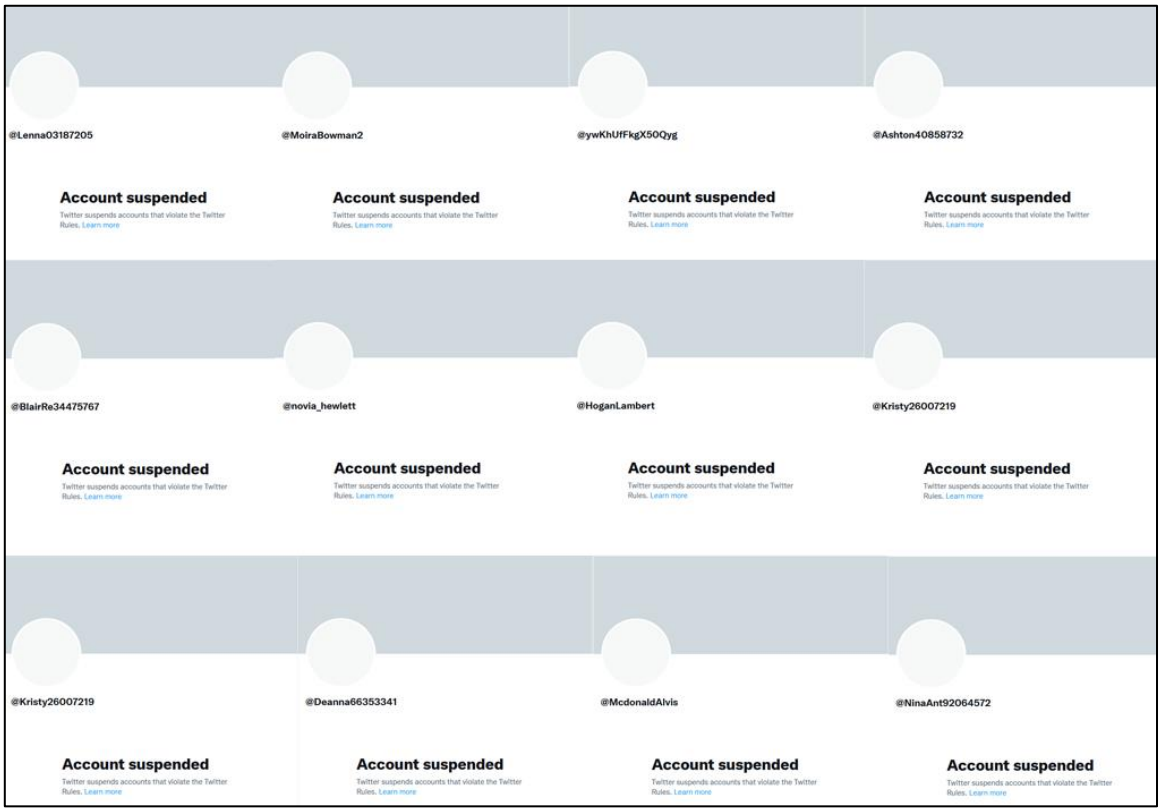


This spam network was also found to be tweeting in Chinese. The aim was to reduce the chances of the appearance of actual news about the protests in case anyone tried searching about it in the Chinese language. Many accounts also posted 18+ content as shown in the following sample collage.



Rate of Attrition

Spamming social media is a tricky business. Given the nature of bots/spam, it's not easy to continue operating smoothly. For example, a large number of the accounts of this spam network keep getting suspended by Twitter. However, these accounts continue to exist and operate in bulk. Extracting the data of tweets over two days led us to identify such a huge spam network. The fact that the activities of these spam networks multiplied by thousand times indicate that they can generate far more accounts than Twitter can suspend.



Even if they get suspended, such accounts continue to pop up and continue their spamming operations. Such accounts are either newly created or are kept dormant for months or years and only come to life when their spamming service is needed as observed after the fire in Ürümqi, Xinjiang, and subsequent protests against the zero-COVID policy by the CCP.

This case study is not a one-time phenomenon that these spam networks are activated to hijack the outgoing news flow from China. To reiterate, these accounts have been existing over the years and operate on a day-to-day basis. Such spam operations are a part of the Chinese social media war against the West and control narrative in favor of its establishment.

On normal days, these spam networks are found to be promoting pro-China, pro-CCP narrative. Their traits and operations patterns have a huge say that they tend

to follow a toolkit and a set of contents is supplied to them daily for spamming purposes.

The traits of these spam networks vary from promoting beautiful pictures of China to using pictures of models for a wider reach to sharing political posts in a coordinated manner, all in mass numbers. The following case study deep dives into one such spam network that was operating with impunity from Twitter's anti-spam surveillance before some of them were suspended, while some continue to operate.

Part II: "Beautiful China": a Case Study in Deception

A coterie of pro-China accounts has been actively operating on prominent social media platforms in a quest to project China in a good light. These accounts work in a concerted manner in clusters and are part of a spam network composed of bots, fake IDs, and amplifier accounts.

But why are we referring to this cross-platform network as a spam network? Diving into the basics, spam is unsolicited content shared in bulk. This particular tool is the essence of this spam network. Due to the prevalence of social media spam, it appears that users will eventually come into contact with it in some way. And hence, it can be assumed that this pro-China spam network operates intending to spread its content in massive numbers to take over a large chunk of cyberspace.

The network is designed to look like individual accounts but each one of its elements mimics the pattern of the other. They operate in a way as if following a certain guideline issued for the purpose. The 'everything China' spam posts range from pictures of scenery, tourist places in China, images of models, and sports.

But a distinguishing feature of this network is that the tweets are infused with political content. The focus subjects of these tweets are pro-China and anti-West political news and opinions. A large number of accounts are bots primarily created to amplify such posts by the other accounts of this network.

Nonetheless, the network is characterized by some obvious signs that their pattern of posting and post sharing gives away. First is that these social media handles use Chinese, and on a few occasions, English language and post-pro-China content in superfluous numbers.

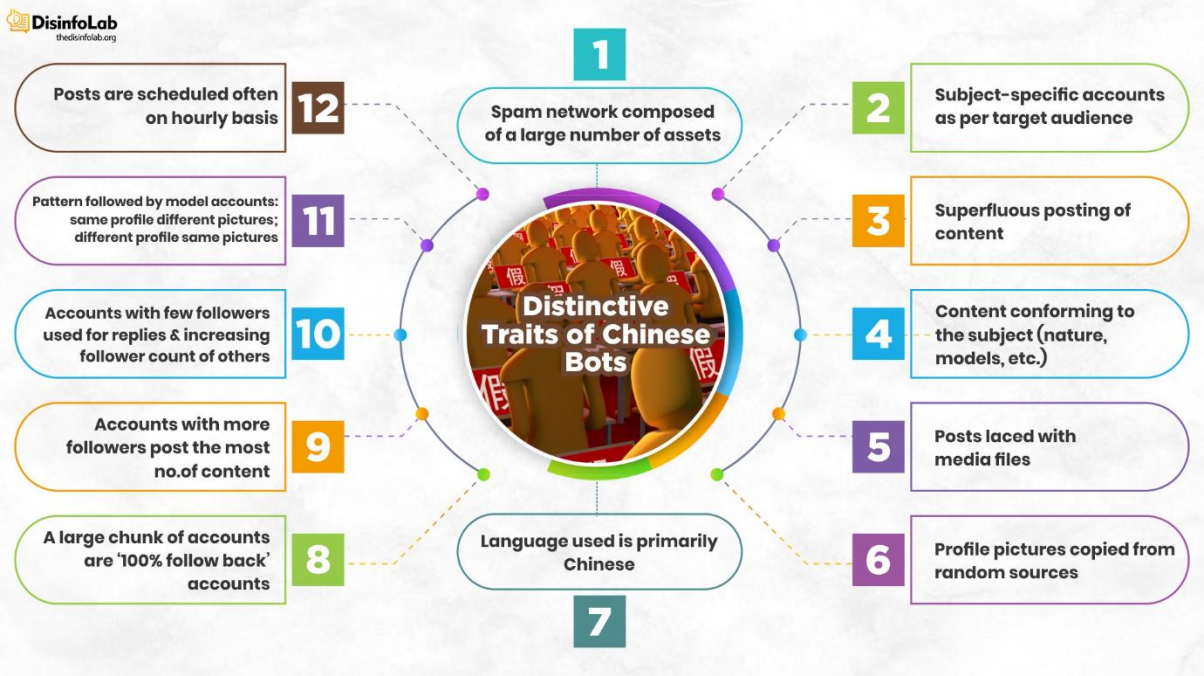
Secondly, these accounts do not garner an organic audience as they receive minimal to no engagement. Some of these accounts, primarily account impersonating models, despite having followers count in thousands, do not even attract likes or comments in more than single digits. This indicates that most of the followers of these accounts are bot accounts.

Another feature is that, as these accounts start posting political content, it is done in a series as if maneuvered by a set of shared guidelines. It is then followed by a chain of retweets and quote tweets that amplify those posts.

Since they appear to have no interaction with each other via commenting or liking each other's posts, it is a cinch to set up an impression of individuality.

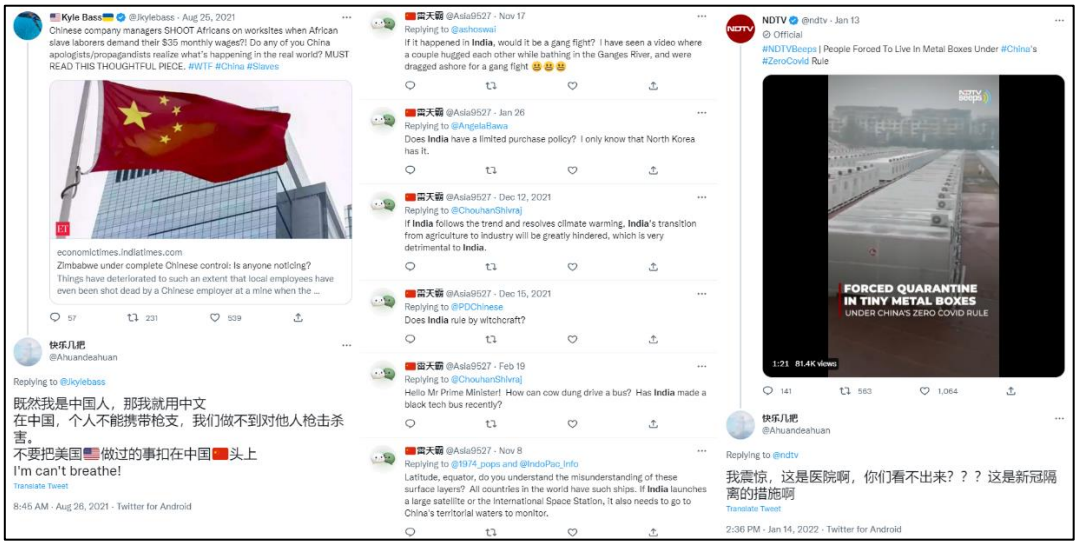
The impact of this spam network and its achievements cannot be gauged fully yet. But what we did find out is that it is working on a massive scale, and interestingly, there is also the involvement of state-sponsored media.

Analyzing their behavior pattern indicates that this network was thriving on a toolkit that might have been distributed to them for several purposes including pushing the pro-CCP agenda.



A Pro-China propaganda social media network

We first identified this cross-platform pro-China spam network while searching the keyword “Beautiful China”. During our investigation, we identified a subset of accounts that run this spam network like a well-oiled engine. While some of them were posting oodles of photographic and video content to mask the promotion of pro-China content, others were involved in attracting traction by posing as models. While there were more of them whose only task was to extend their reach by participating as repliers of random posts.



Section A: Beautiful Propaganda

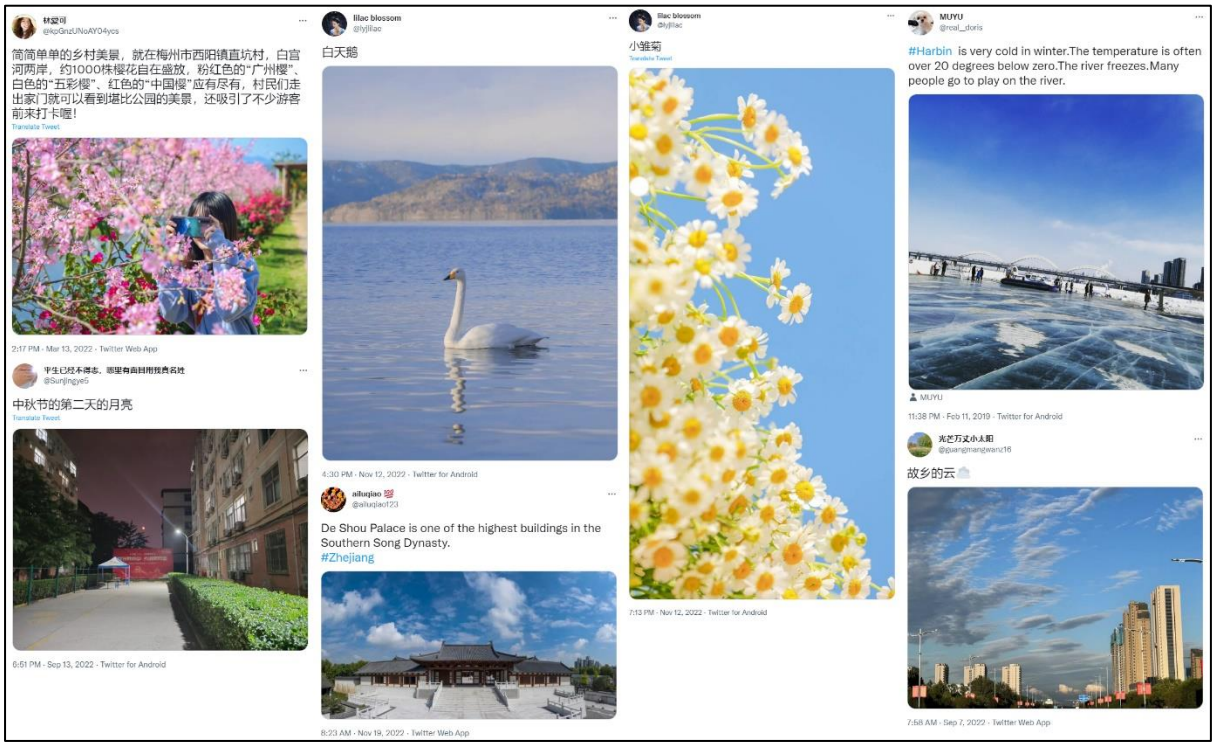
While studying this massive-scale spam network, we came across accounts that mainly posted aesthetic pictures of scenery and photographic content across their social media platforms. On the face, these seem like normal accounts, but a careful examination of these accounts reveals that aside from the random spam posts they posted pro-China content.

To demonstrate the pattern of their posts, here is an example of an account @guangmangwanz16.

Non-political spammy posts content uploaded by @guangmangwanz16

Political content praising China and promoting China-affiliated media posted by @guangmangwanz16

The other accounts from this network were mimicking the same pattern. We extracted several common traits among these accounts that characterized this network. To begin with, the majority of these accounts had followers above 1k, most of which comprised '100% followback' accounts. Despite that, the engagement was abnormally low. Many of these accounts followed each other while some quote-tweeted each other. However, no interaction in the form of likes or comments was observed.



Another pattern detected in some other accounts was their role in retweeting Chinese media content, both political and non-political.

An account @binghe47197208 was found to follow a particular pattern of retweeting and replying. The majority of tweets by this account were composed of retweets, not to mention, the exuberant number of tweets per day. The account was created in May 2022 and so far, it has crossed over 15K tweets. The daily average of its reply tweets in China is around 50 and that too with a just a “thumbs up” emoji. To sum up its activity, the account retweets any China political/development tweet, likes its tweets, replies to them, and likes the reply as well.

An important pattern that we picked up was that while the frequency of political content remained low when done by the accounts, it was done in batches. This indicated the possibility of a toolkit that could be followed by these assets, which we will discuss in the subsequent sections.

A point worth noting is that the assets of the network equip their tweets with media. A minuscule proportion of the tweet is only text while the focus is on using as much media as possible for its further circulation via quoting tweets.

The major goals of this network were obvious. To draw the veil on its political post-sharing pattern and leave imprints of themselves in the social media space as much as possible. For doing so, the network has been continually expanding its assets.

Section B: A 'Model' spam-network

Speaking of a fabricated network, the second set of accounts that we extracted was fake handles posing as models and social media influencers. These accounts were replete with images of models and random pictures of food. But among them, they have also been posting pro-China political content, minimal in number though. But that is precisely the image they aim to create. An image of a normal account with no goal of propaganda peddling.

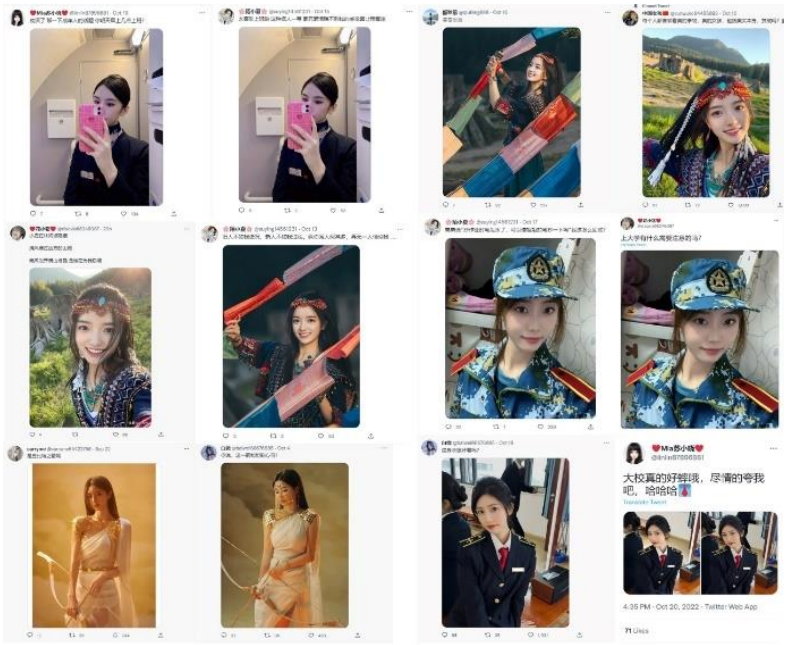
These model accounts, to go by their nature, use pictures of models as their identity and content. Another goal seems to be the gain a large number of followers.

As we analyzed some of these accounts, we chalked out the major characteristics displayed by these accounts: Most of these accounts were newly created, mainly

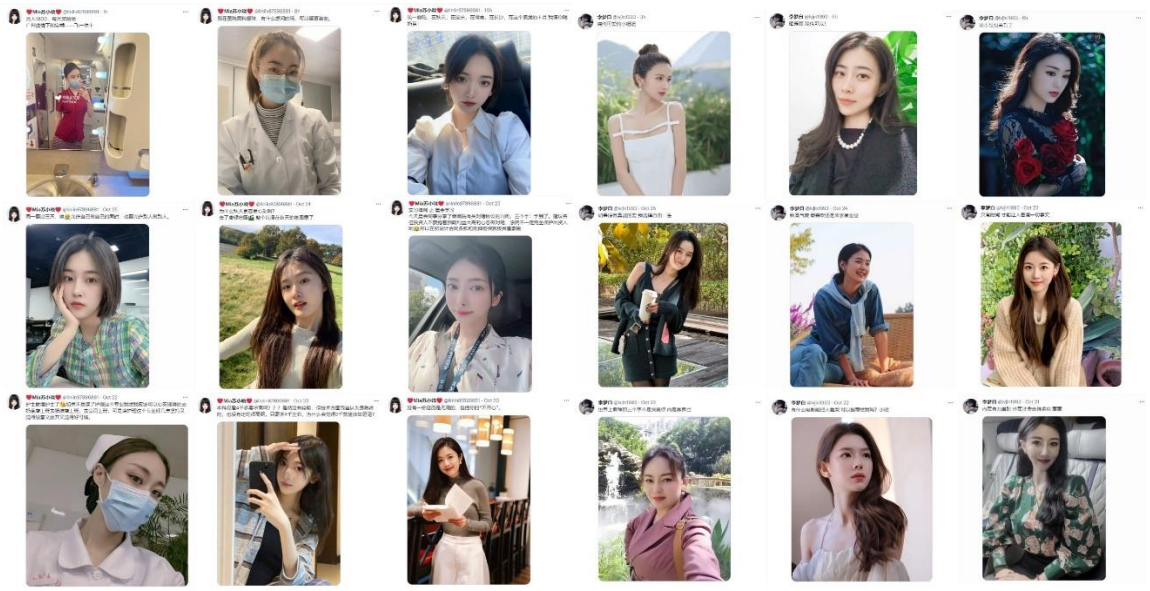
in 2022. In addition, they had a decent number of followers count, somewhere in the thousands. However, despite that, the engagement on their posts didn't seem to be as much as one would expect from an account with these many numbers of followers.

Furthermore, there were inconsistencies between the pictures posted by these accounts with their display picture. Major giveaways of the IDs being fake were the usage of different pictures of models posted by the same account claiming to be an individual. Additionally, there were other accounts there were strings of other accounts that were posting the same pictures.

A similar pattern was observed in hundreds of such model accounts of this spam network on both Twitter and Facebook.



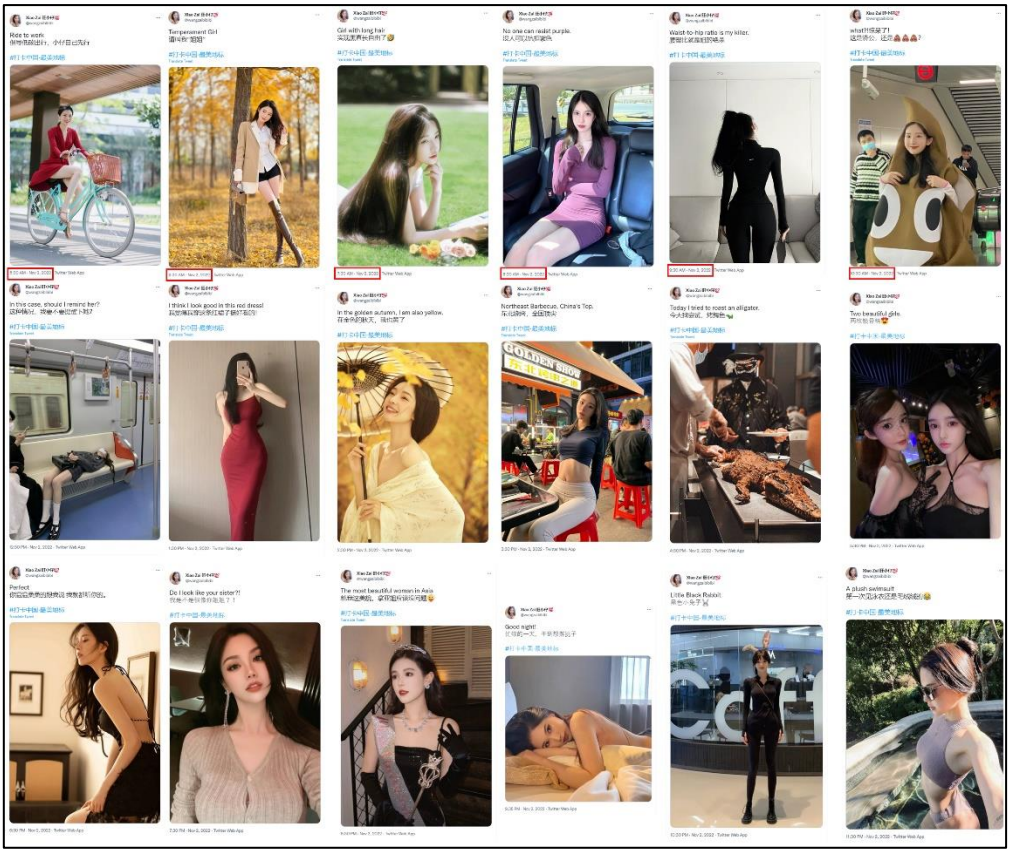
Different accounts using the same pictures of models



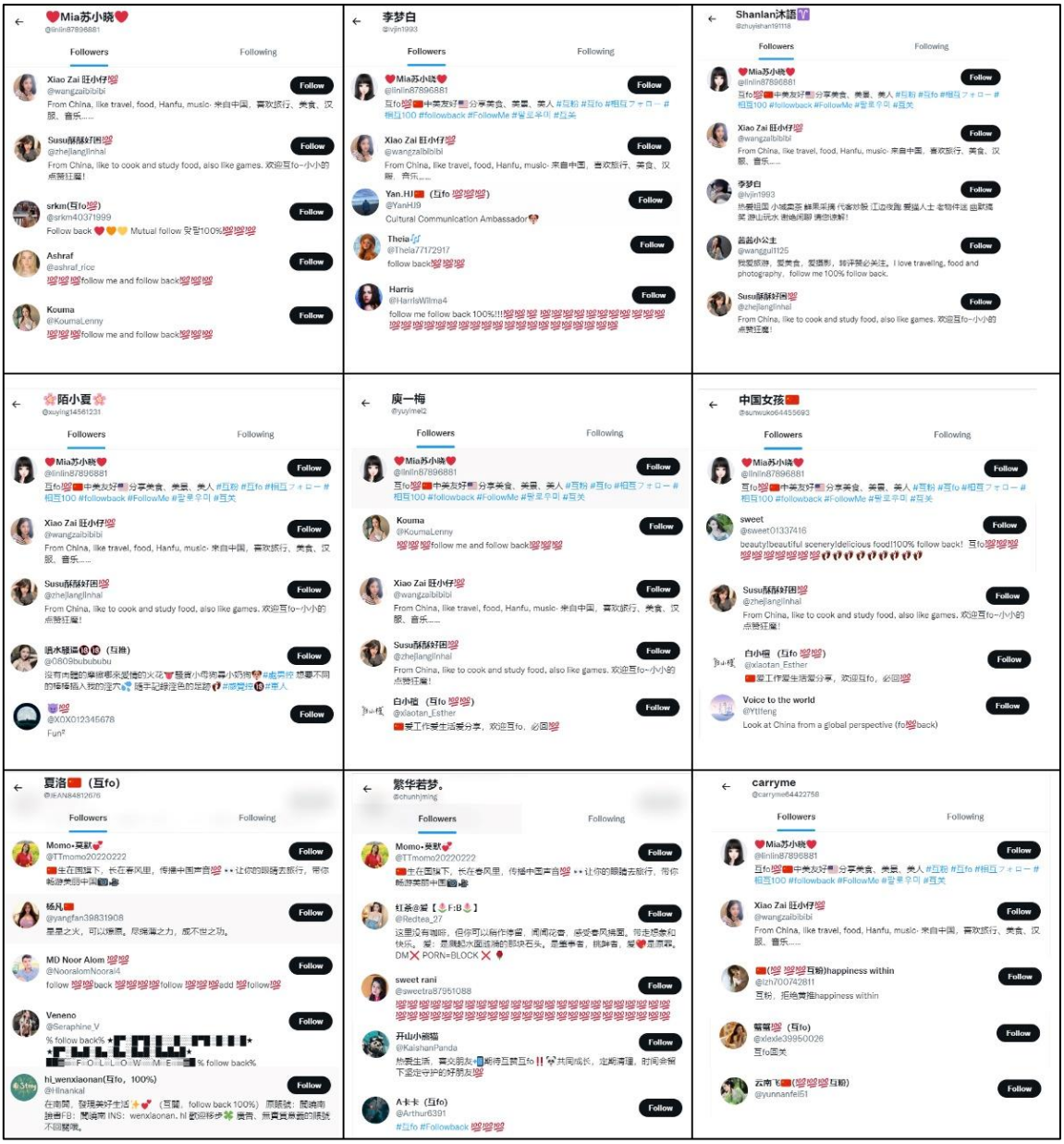
The handles @linlin87896881(left) and @lvjin1993 (right) post pictures of different women

These accounts have a clear telling of their spamming behavior, it was also observed during our investigation that most of them were working in an automated manner. We identified accounts that were posting pictures and tweets on an hourly basis.

For instance, two such handles @*wangzaibibibi* and @*Linlin87896881* were found to be spam-posting pictures every hour as if it was their posts were scheduled by any software.



And while analyzing the followers of these accounts, we found that the list was replete with “100% follow back” and similar “model” accounts exhibiting the same behavioral pattern.



Followers comprising 100% follow back accounts

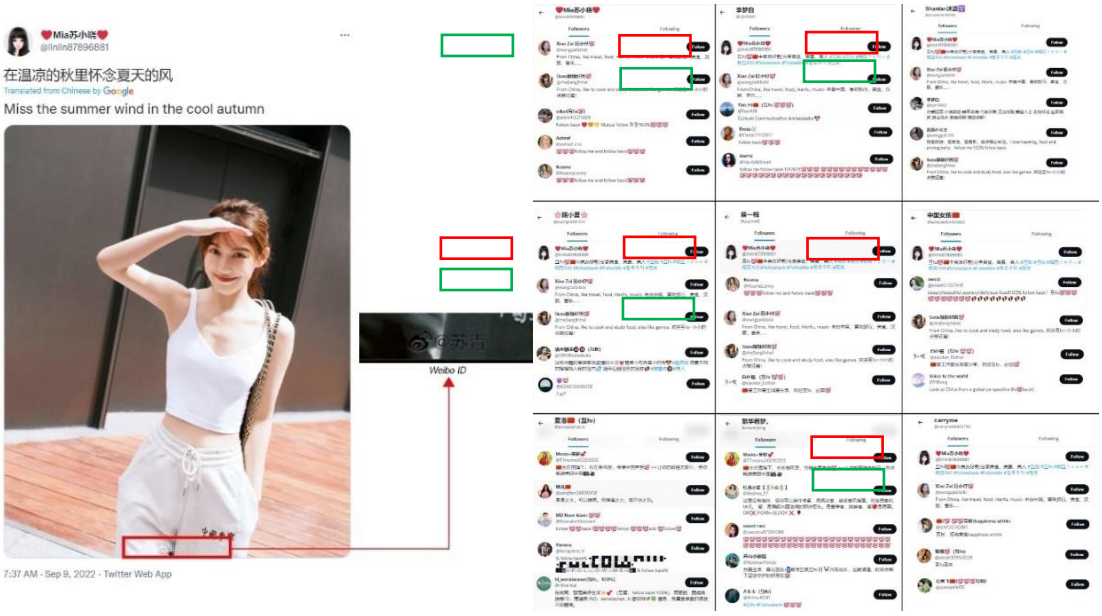
Section C: DP borrowing network

As mentioned, the model accounts form part of this network and operate with an assumed identity. And a key part of this practice is either picture theft or using pictures of prominent models or actors as the display pictures by these spam network accounts. While analyzing the followers' list of these model accounts, we observed several accounts following the same practice. From these, we identified seven such accounts.

One case is the Twitter account @*wangzaibibibi* which claims to be a Chinese citizen. However, the display picture used by this account is of a Korean actress, Shin Ye-Eun. Her picture was taken by this spam network account from one of the fan pages of the actor.

The graphic below shows the display picture put up by @*wangzaibibibi* and the origin of the picture.

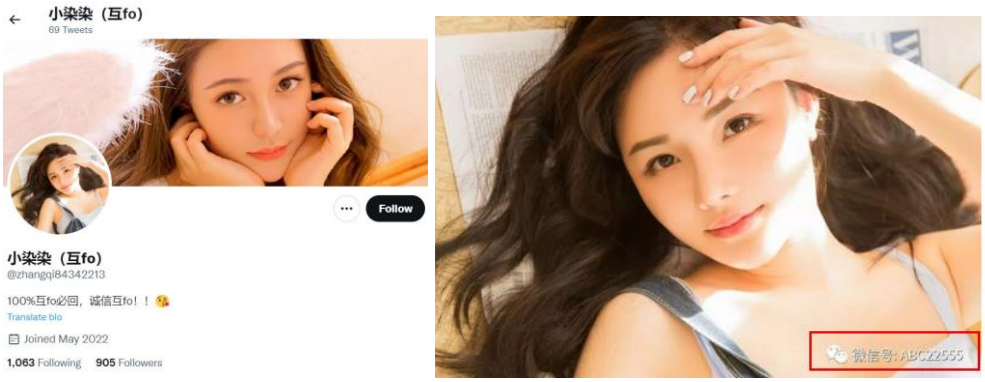
The second case of DP theft was observed in a '100% followback' account *@linlin8789688.* This account had acquired the image from a Weibo user as depicted in the graphic below.



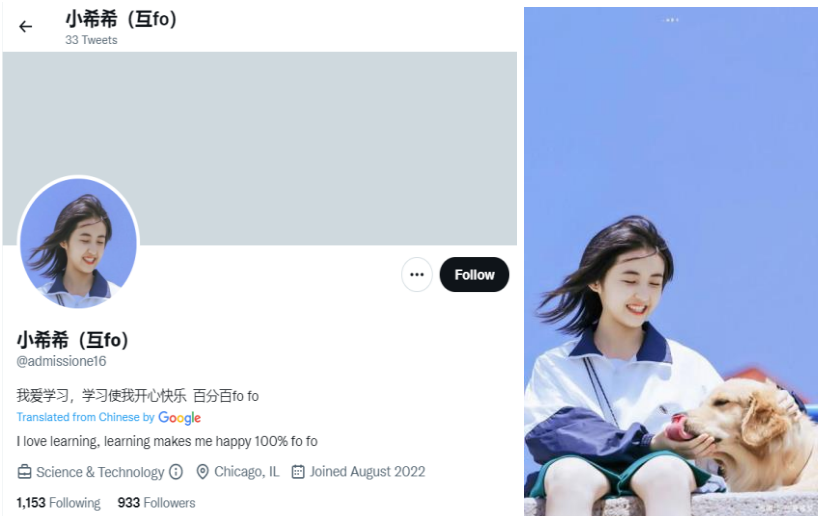
(Left) Account @linlin87896881 picture taken from a Weibo account mentioned in the picture. (Right) Graphic showing @linlin87896881 (marked in red) and @wangzaibibibi (marked in green) as common followers of the fellow fake model accounts of the network

In other cases, it was observed that these DP stealing accounts were obtaining images from random sources such as adult websites, social media platforms like Weibo & WeChat, and movie clips.

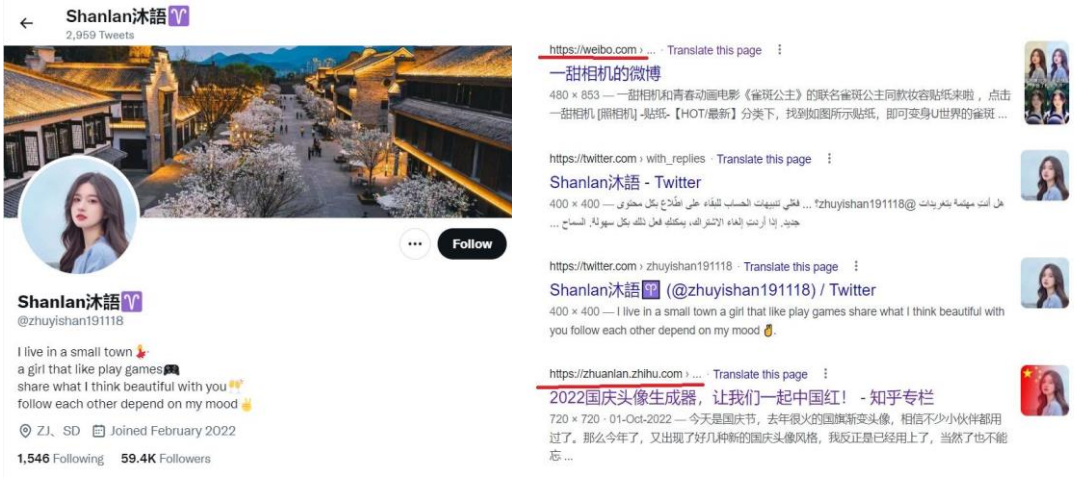
The graphics below depicts three more cases of DP theft accounts.



(Left) Twitter account @zhangqi84342213 and (right) source of its display picture



(Left) Twitter account @admissione16; (right) displays a picture used of Chinese actress Zhang Zifeng from one of her movies



(Left) Twitter handle @zhuyishan191118 and (right) source of the used display picture

Apart from the shared trait of DP stealing, these accounts had a common trait of being a 100% follow-back account as discussed in the preceding paragraphs.

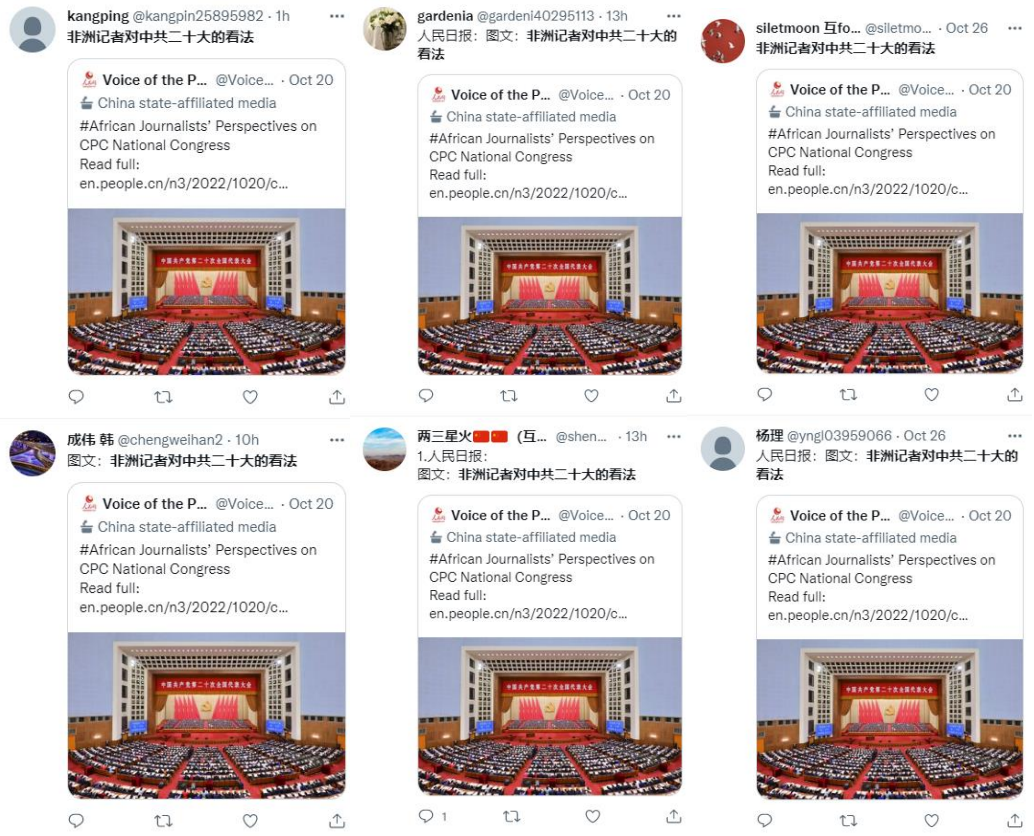
Section D: A dissociated communication

A common behaviour observed in another set of accounts was that they were essentially carrying out the task of quote tweeting and retweeting. These bot accounts were quote tweeting the same posts in a tandem manner, working as amplifiers.

A specimen of such a bot account is @zhangdo09042397. Scrolling through this account, it was evident that barring Facebook links, this account profusely shares China-affiliated media posts. The rate at which this account retweets such posts ranges from 4-7 per day.

Posts of account @zhangdo09042397 quote tweeting China-affiliated media content

Searching the same text from one of the quote tweets by this account revealed a plethora of other bot accounts sharing the same post. This was not done necessarily at the exact time but in a similar timeline. Perhaps to ensure that the spam content lingers in the cyberspace for a longer period.



Another pattern observed in these bot accounts was the sharing and resharing of the posts in excessive numbers per day. This clearly indicated a typical pattern of spamming.

Section E: A Link-sharing Kinship

Apart from sharing the same set of political tweets, the connection between the bot accounts was also revealed by their common pattern of sharing the same Facebook links. Moreover, these accounts displayed an abnormal like-to-share ratio.

A representative example of how this bot-sharing network works is that of a broken Facebook link shared by a user *@QT43191380.* A cursory look at the activities of this account gives away that it is created for mainly retweeting China state-affiliated media tweets. Other than that, it posts Facebook links, which are mass-shared by bot accounts.

One of the FB links shared by this account was a broken one. Even this link was shared extensively by these bots on successive days, ascertaining their automated behavior.

Broken FB link posted by the account

Broken FB link posted by @QT43191380 shared by bot accounts

Manually going through the profiles of these accounts, it becomes apparent that their sole purpose is sharing links, most likely provided by a toolkit, and promotion of Chinese-affiliated media houses.

We picked up two accounts from this bot network that demonstrated their behaviour. The timeline of the Twitter accounts *@Ava34290917 and @yaya90710791* revealed that they were prolifically involved in the propagation of Facebook links and Chinese-affiliated media houses.

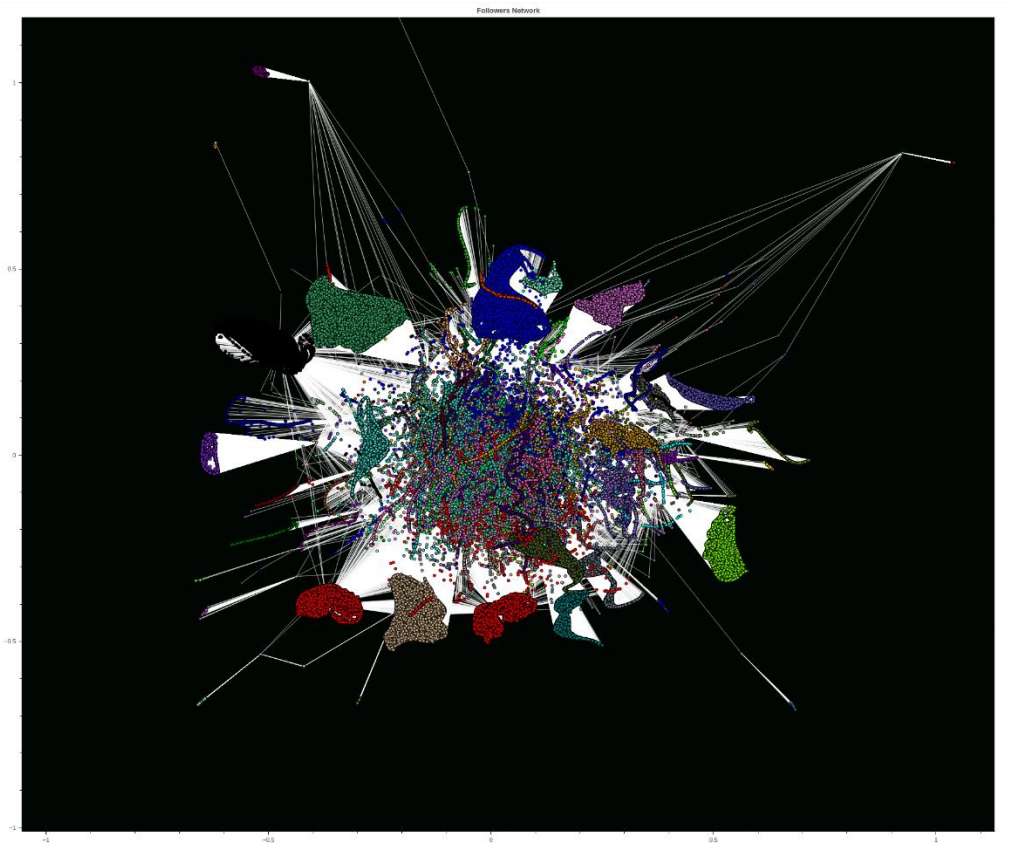
Tweets by two accounts @Ava34290917 and @yaya90710791 sharing FB links (top) and China state-affiliated media content (bottom)

Part III: Twitter Analysis

On the face, these accounts seem to work disjointly and in isolation. However, in contrast, they were found to comprise a vast network identified via their followers' and following pattern. To reiterate, these accounts were seen to be sharing posts with zero/ negligible engagement to show that they are not working in conjunction. However, the investigation of these 140 accounts, indicated a vast network of 2,61,658 accounts that follow each other and with the salient features as elaborated in the previous sections.

The following graph shows the number of accounts and their followers' networks in clusters. Each cluster and its nodes are the same in color and different from the other set of clusters and their nodes. This signifies the unique followers of the accounts in the graph.

To simplify, each cluster and its nodes depicted by the same color indicate the unique followers of each cluster that are different from the followers of other clusters.



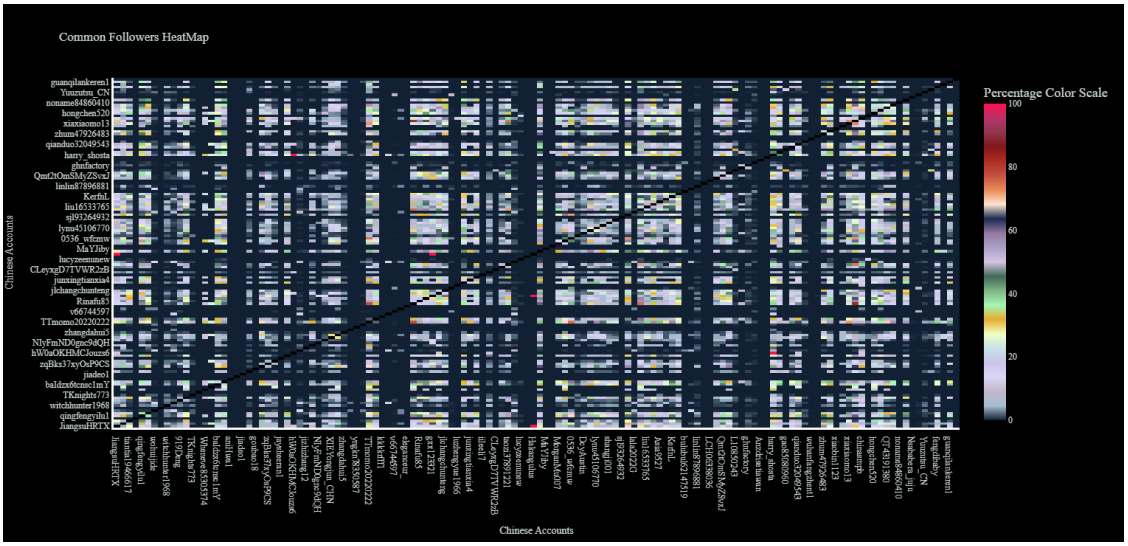
However, many nodes depicting the followers also assemble at the core of the graph in large numbers. This is to explain that these are the common followers of all the accounts of the whole network. Even a cursory look at the core tells that the

common followers' network is much larger in number than the unique accounts depicted in each cluster and their nodes.

This explains that even if these accounts don't engage with each other, they do share common followers with the automated traits explained in the earlier sections.

As depicted in the following graph, the number of common followers of the accounts of this network is in a large proportion. The band between the x-axis and y-axis represents the common followers of all the accounts. The usernames of the accounts that are plotted on the 'X' and 'Y' axis respectively shared the common followers among each other.

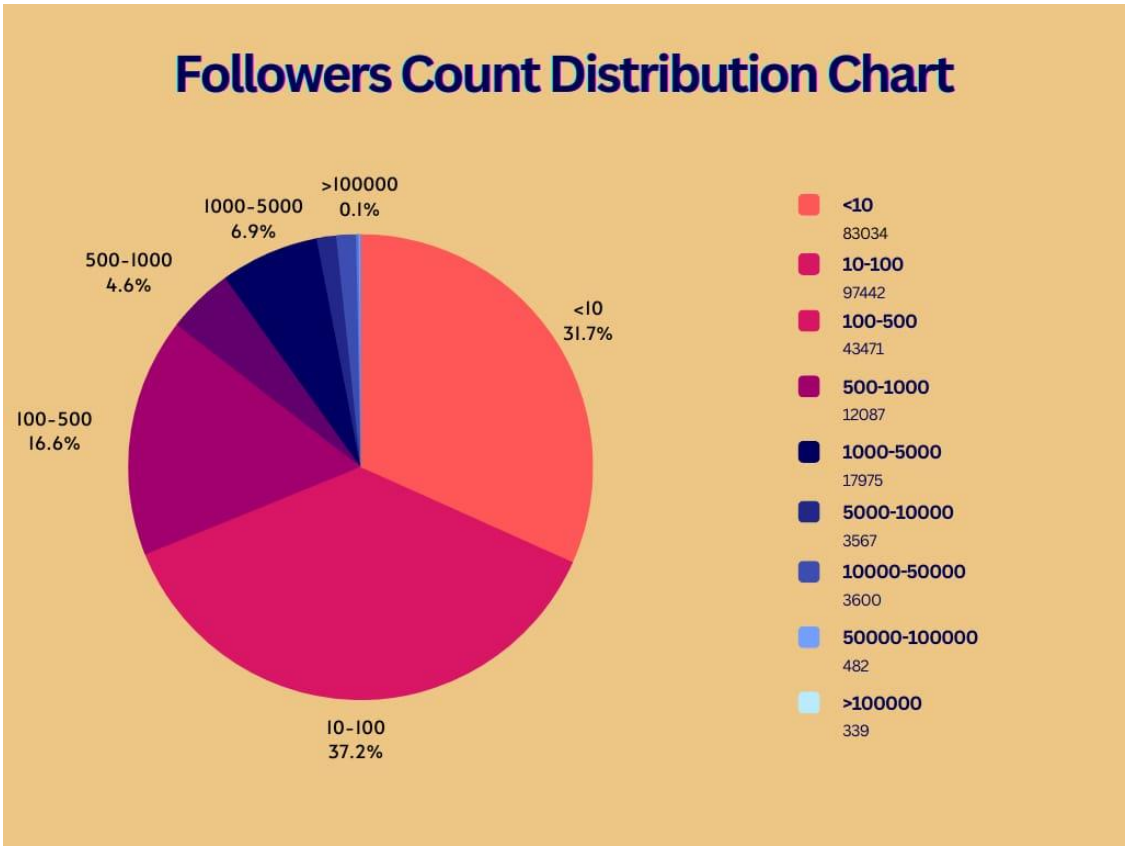
The common followers of the accounts are denoted in percentage and signified in colors on the Y-axis. This explains that one of the core objectives of this network is to grow each other's accounts by following each other even though they don't interact on social media.



To further explain, we plotted the pie-chart of the followers' count distribution to understand the segregation of the accounts' followers, their nature, and their purpose and we noted that:

- A total of 37.24 % out of 2,61,658 accounts had followers ranging below 10. Implying, that these accounts were primarily created to increase the followers of their fellow accounts in the network.
- A total of 31.73 % of accounts had followers ranging between 10-100, which were recorded to be sharing scenic pictures of China to spam social media.

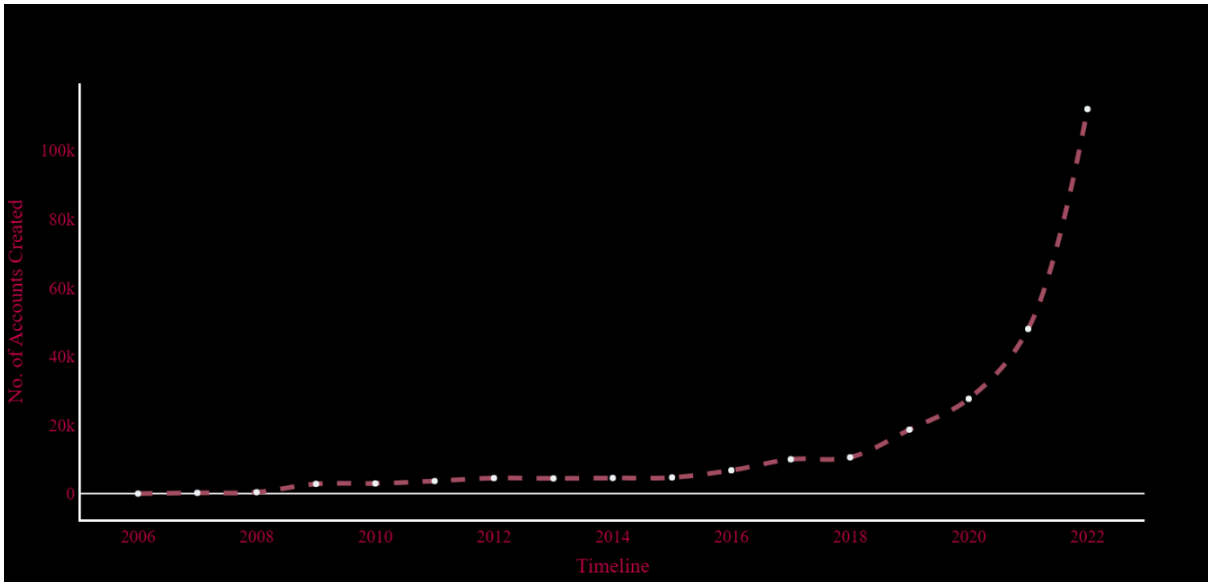
- And the rest accounts with followers ranging starting from 1000 signified the model accounts which were again gaining followers rapidly and were also spamming on a pattern hourly basis (elaborated in Section B).



The Motive

These accounts have been active for a while and have been effectively operating to accomplish their goals. If one were, to sum up their agenda, it is to acquire dominating presence on social media so there appears only positive content surrounding China.

Their role varies from spamming to sharing pro-CCP posts and even promoting pro-China narratives on Twitter and cross-platforms. The existence and activity of these accounts on social media platforms, Twitter and Facebook, can be seen surging from 2018 to the present. The following graph shows the accounts' creation timeline showing that a total of 10,571 and 18,647 accounts were created in 2018 and 2019, respectively.



Accounts' creation timeline

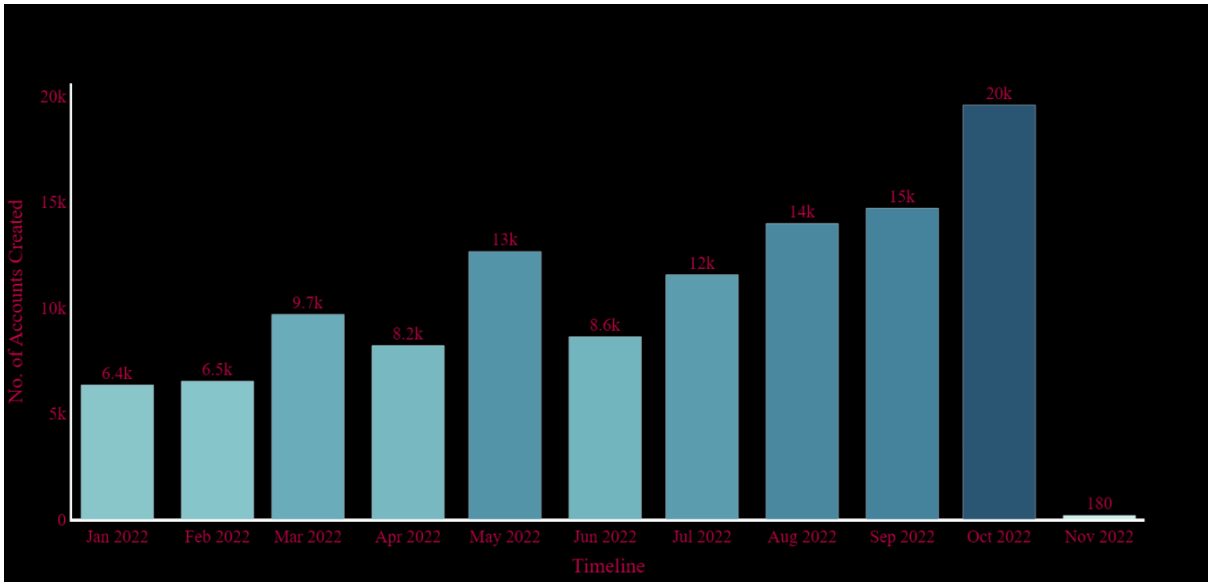
However, the accounts created increased almost two-fold to 27,625 and 47,988 accounts in 2020 and 2021, respectively. This can be easily explained as, during these two years, China was at the center of criticism for the COVID-19 virus origin.

However, in 2022, the accounts' creation multiplied three-fold as compared to 2021 and saw 1,12,067+ accounts being created alone. These can be explained by two major events that took place in 2022:

a. The 2022 Winter Olympics
b. The 20th National Congress of the Chinese Communist Party (NCCCP)

Beijing won the bid for hosting the Winter Olympics on July 31, 2015, and successfully hosted the event from February 4-20 this year. [7] We observed that many accounts that were posting pro-China content on Twitter were created around the event as shown in the following graph.

[7] https://olympics.com/en/olympic-games/beijing-2022



The account creation of this network did not stop, instead, it increased from July onwards and peaked in October. The 20th NCCCP opened on October 16 and closed on October 22, 2022, in which Xi Jinping secured his third term as China's President. [8]

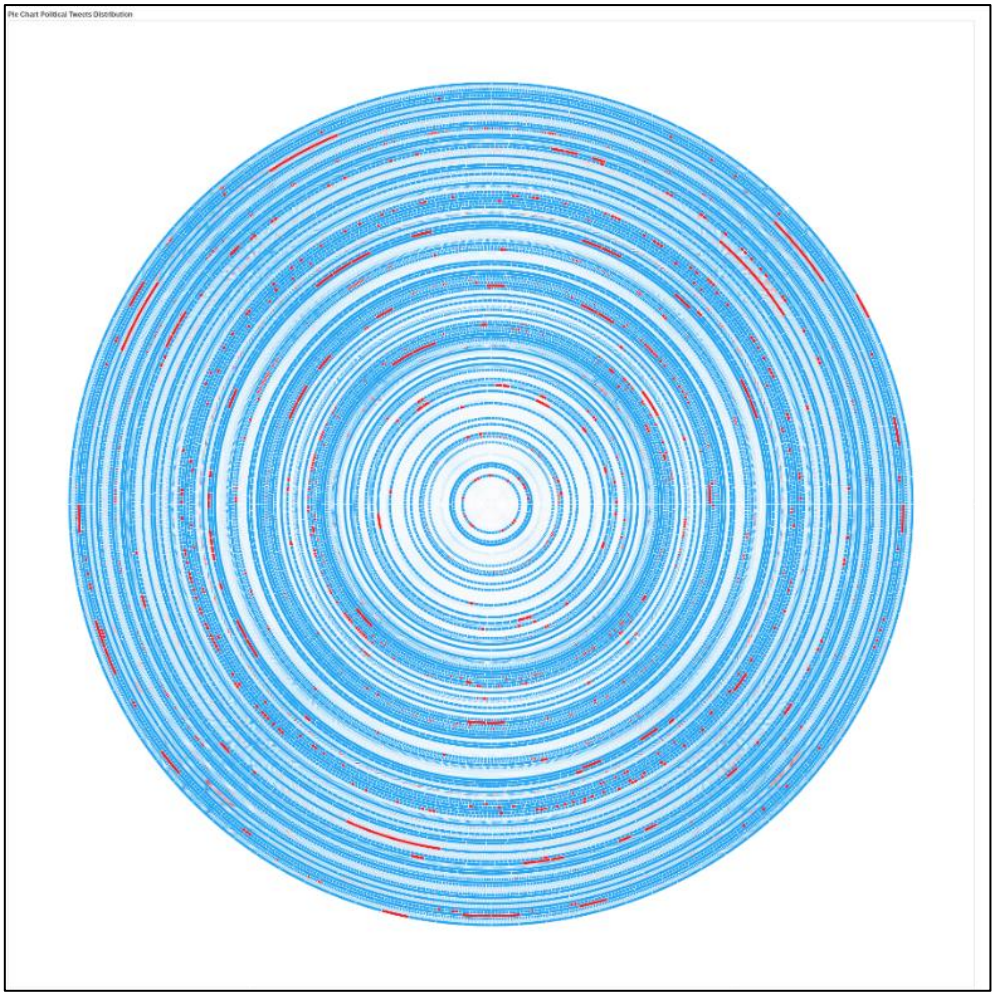
Many accounts in this network were found to be promoting pro-CCP content around and after the 20th NCCCP while spamming the platform.

Having already established that a large number of these accounts were created in 2022, we looked at the timeline of their posts. It was found that these accounts mimic each other in the type of content they share. Moreover, it is almost as if like they are operating parallelly.

The accounts involved in this spam campaign work in a concerted manner. As pointed out in the previous sections, while a high proportion of their posts are non-political posts in Chinese, when they do post political content, it is done in a series.

To get a better insight, we plotted a circular graph of their post-sharing activity. The below graph shows the frequency of the political posts shared by the assets of the spam network. Each concentric circle represents an account. The blue-colored blocks depict non-political posts, while the red ones represent political posts. As is evident from the graph, we can see streaks of red which depict that when political posts are shared, they are shared in batches. This behavior was common among these accounts.

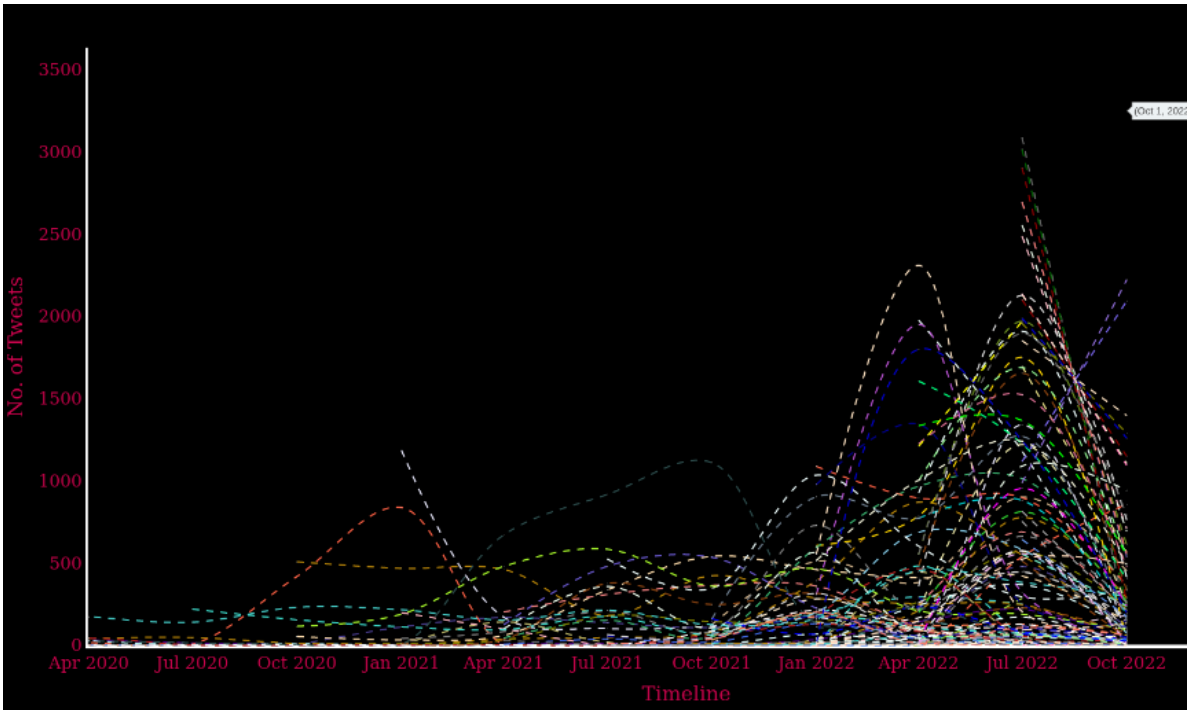
[8] https://www.indiatoday.in/world/story/china-president-xi-jinping-re-elected-third-term-general-secretary-communist-party-2288597-2022-10-23



Frequency chart of political tweets

The activity of this network suggests that they work in a concerted manner. The below graph shows the timeline of these tweets. The peaks in the graph depict the timeline of the activity of the tweets since 2020. The waves and the peaks coinciding with each other suggest that the accounts have been active around the same timeline. They also follow a similar tweet pattern when it comes to political and non-political tweets.

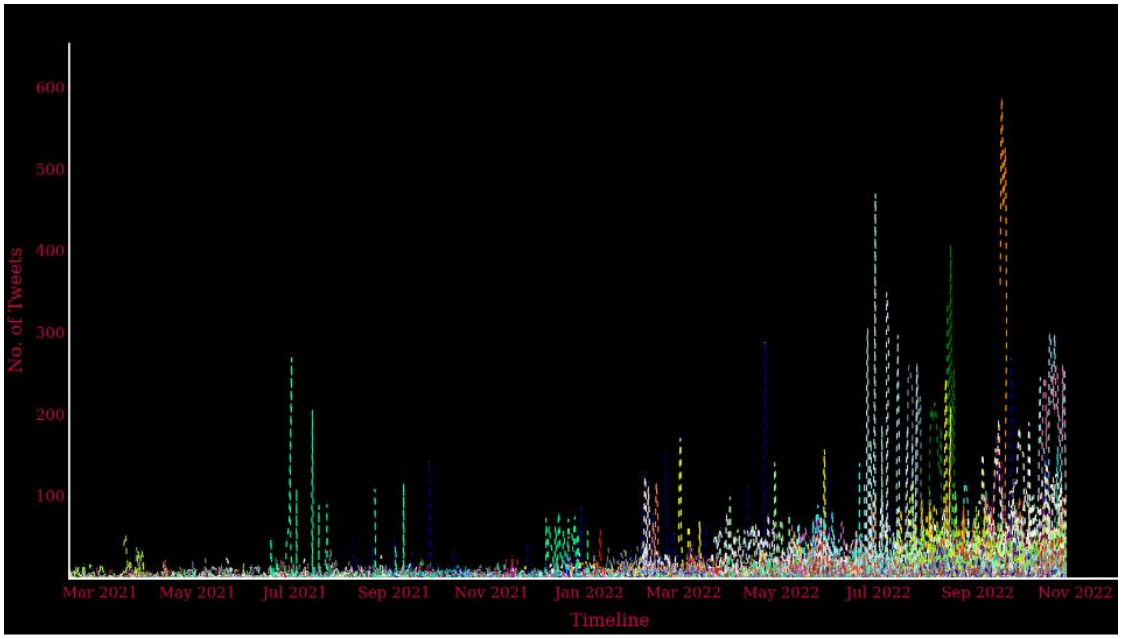
The activities of these tweets have increased since January 2021 and reached a peak in the third quarter of 2022. Although the tweet numbers may vary, the graph is a clear indication of them working in a coordinated manner. Meaning, when they are posting non-political tweets, they are doing it around the same time. A similar pattern has been seen in the posting of political tweets.



Graph showing quarter-wise timeline of tweets

The second graph gives insight into the day-wise timeline of the frequency of tweets. Two key observations can be made from this one that proves the point of the quarter-wise timeline graph. The bunch of spikes represent the multiple accounts. The mixed color pattern, spikes coinciding with one another, shows that these accounts have been following a certain routine in their social media activities. This pattern surfaces when the network amplifies their political tweets and they do it almost together.

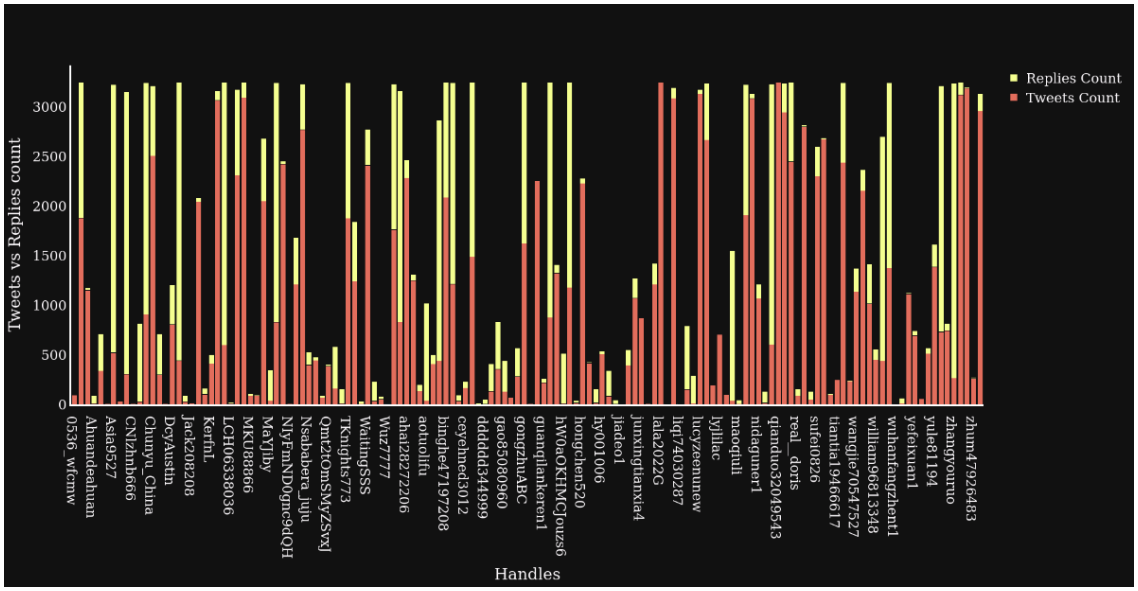
This particular pattern is indicative of bot-like behavior and solidifies our observation of the same. Another key point is that, as we mentioned earlier and as was observed in the political tweet frequency pie-chart, the post pattern suggests the involvement of a toolkit. It can be deduced that while the accounts are not actively posting political tweets, that is to say until they receive the toolkits in question, they are left to post all sorts of spam content.



Tweets timeline day-wise

The Reply Army

Additionally, we noticed that several accounts were primarily engaged in replying to random posts by other accounts. This number is unusually high, which is consistent with the finding that a lot of accounts were used to reply to other tweets to spread their presence. A graph depicting the tweet-to-reply ratio of some of the accounts of this network is displayed below.

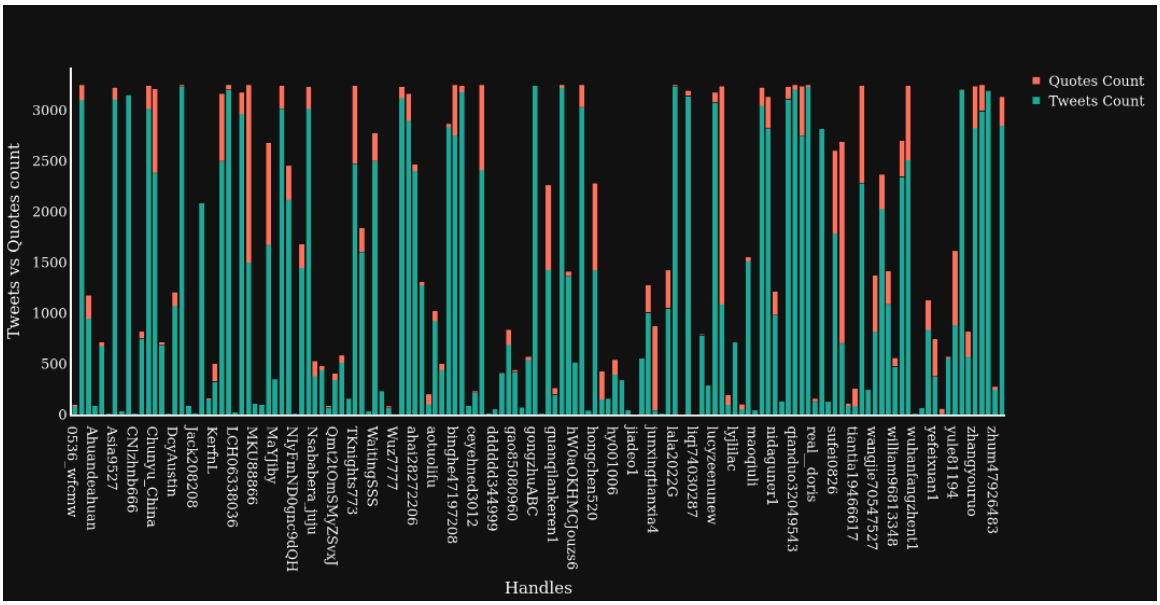


Similar to how some of the accounts posted several posts per day, these accounts mirrored the frequency of replies. An example of this behavior can be seen in the account @zhangyourou. A look at the tweets by this account shows the number of posts ranges between 3-14 per day. A maximum number of these tweets comprised replies. For instance, on October 25 alone, this account made 12 tweets out of which seven replied to other posts.

(left) Tweets made by @zhangyourou on October 25 and (right) a general look at the nature of tweets by the account. These images show that the tweets are predominantly comprised of replies

The Quote masters

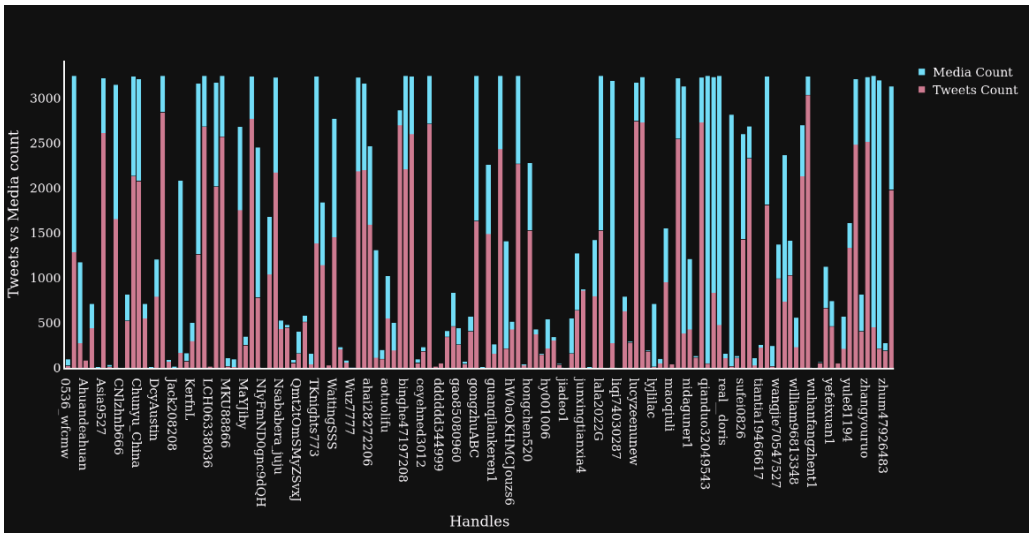
As noted in previous sections, a large proportion of the accounts were involved in quote tweeting, primarily political content. The graph below draws a comparison between quote tweets and original tweets done by these accounts.



Graph depicting Tweet vs Quote count

The Media abundance

If there is one obvious observation that anyone visiting these accounts can make is the abundant use of media files in their tweet posts. As the graph shows, there is a fairly small difference between tweets and media count. The undeniable reason behind such profuse use of media is to conveniently conceal the presence of political tweets. A greater number of media also makes their spamming operation more efficient.



Graph depicting Tweet vs media count

Part IV: China-Pak Propaganda

The role of the Chinese spam/ bot account network is to ignite propaganda on social media. In such cases, what usually follows is either planting fake news/ or fake media by an anonymous bot account, later to be picked by other handles for the amplification purpose. Such a case was witnessed recently around the National Congress of the Chinese Communist Party (NCCCP) in October 2022 when a Chinese bot account posted a video of the 2020 Galwan Valley clash between the Indian and Chinese armies. The video was later picked by Pakistani social media to further the Chinese propaganda against India.

Putting Resources to Good Use: Galwan Valley Skirmish

The border dispute between India and China in the Himalayan region has worsened in recent years. The disputed region is also known as the Line of Actual Control (LAC). The two Asian powers have gotten into skirmishes on numerous occasions, which have reverberated the ties between India & China.

The pick-up point of the skirmish over the territorial dispute was on June 15, 2020, which was particularly violent. It was the first fatal confrontation of both armies since 1975 in the Galwan Valley. While the fatalities were reported on both sides, China refused to release the number of casualties on its side nor did the country comment on reports claiming a high number of casualties on its side.

According to the Australian newspaper Klaxon, which cited a report curated by a group of social media researchers on the Galwan clash, Beijing tried to conceal the actual number of casualties. Beijing went beyond the extent to silence the discussions of the Galwan clash & even deleted videos & reports around it.

But what was more important to note was China's never-ending propaganda on the clash. And while this was a sensitive issue for both involving casualties on both sides, the two countries engaged in rounds of military talks to resolve the LAC issues. The conclusion on common grounds is yet to happen (as of October 2022), the propaganda was an option to prolong this border dispute.

20th National Congress of CCP & Propaganda follows

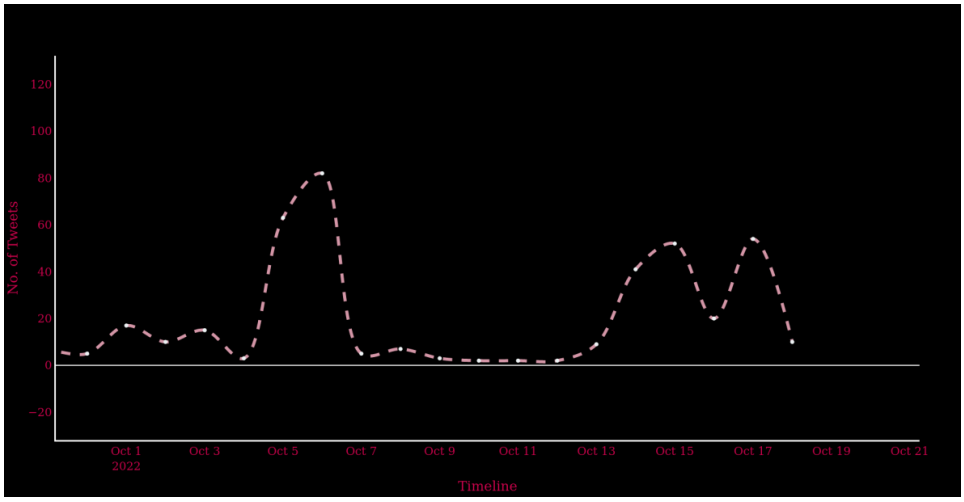
China observed its 20th National Congress of the Chinese Communist Party (NCCCP) on October 16, 2022, which is held every five years. This is the time when Chinese propaganda tools and troll farms get busy exemplifying the countries' laurels. And so, were subjects picked for churning pro-China propaganda. The Galwan Valley skirmish became their target and was picked by the Chinese handles around the 20th NCCCP.

Therefore, to deep-dive into how the Chinese propaganda on Galwan Valley unfolded, we analyzed the tweets on 'Galwan' between October 1-18, 2022. The data indicated that it was not just Chinese propaganda but also involved its 'iron brother' Pakistan.

Notably, India's Home Minister's three-day visit to Kashmir commenced on October 3 followed by a high-level meeting on October 5. [9] [10] A total of 4,424 tweets were done on Galwan alone between October 1-18, 2022.

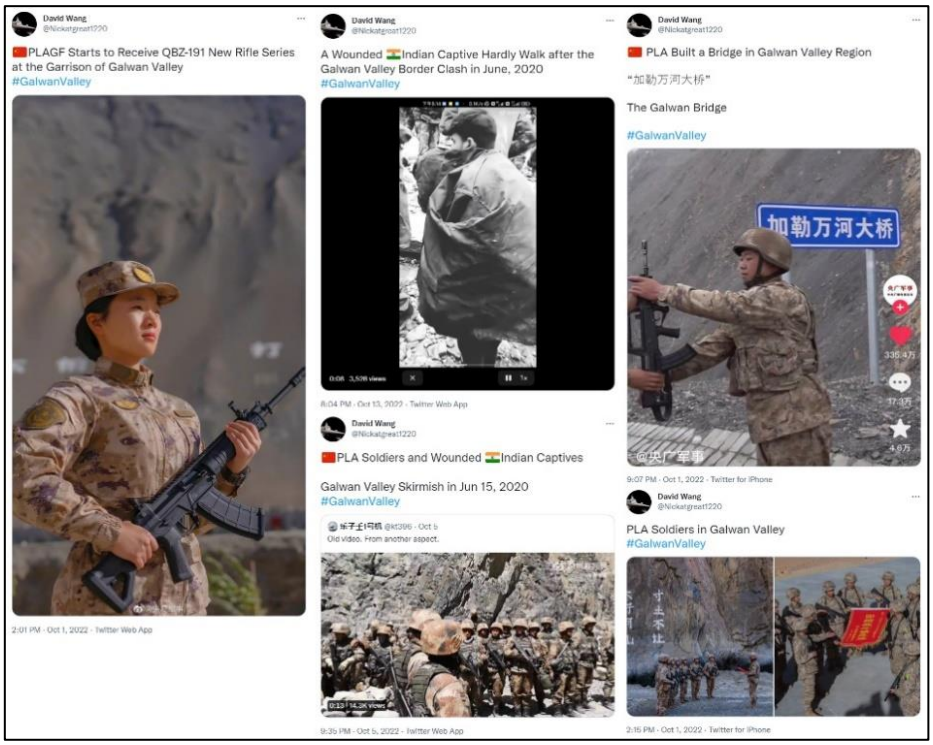
[9] https://newsonair.gov.in/News?title=Home-Minister-Amit-Shah-to-begin-three-day-visit-to-J%26K-from-today&id=448729

[10] https://www.livemint.com/news/india/jammu-and-kashmir-visit-home-minister-amit-shah-chairs-high-level-meeting-in-srinagar-11664953118478.html



The first of many tweets on Galwan was initiated on October 1, 2022, by a Twitter user @Nickatgreat1220 (David Wang), who describes himself as an aggregator of Chinese Military facts based out of Beijing. [11]

@Nickatgreat1220 alone tweeted 120 times on Galwan during this period. However, an important aspect to put an eye on was his amplifiers. One of his earliest amplifiers is a US Army officer Michael Lima.



Michael Lima is a Professional military officer and skilled educator with twenty-three years of experience in logistics management and over nine years of experience as an adjunct instructor. [12]

[11] https://twitter.com/Nickatgreat1220/status/1576127573519568897
[12] https://www.linkedin.com/in/limamike10/

As @Nickatgreat1220 continued to go about his tweets on Galwan, promoting the Chinese narrative, some Pakistani accounts started getting followed by Chinese government officials Libijian, the Consul General of China to Karachi, and Pak-based Chinese diplomat Zhang Heqing started engaging with his tweets. [13]

Several Pakistani accounts also amplified the Galwan tweets by Nickatgreat1120 by retweeting him to promote the pro-China, and pro-People's Liberation Army (PLA) tweets by *@Nickatgreat1220*. [14] These accounts such as @CentralPahk, @AsadRahim, and @HamidouRaiss were also promoting the interests of Pakistan.

In continuance to the pro-PLA propaganda, a Chinese bot account *@kt396* posted an old video of the Galwan Valley clash to show the heroics of the PLA soldiers. [15]

So far, the efforts of projecting PLA in a good light by riding on the Galwan Valley incident were happening in microcosms until October 5, when Pakistan Strategic Forum (PSF) members jumped into the scene.

According to its website, Pakistan Strategic Forum (PSF) is a Pakistan-based thinktank that strives to offer Global News, International Events, and those about Pakistan. [16] It was founded in 2019 by Aanis Kamal, a student of Fazaia Inter College (under Pakistan Air Force), and Umair Aslam, son of a former Pakistan Airforce officer. [17]

But PSF has a history of running propaganda campaigns against Pakistan's neighbouring countries. It was one of the key entities to have peddled the *#BoycottIndianProducts* against India in 2021 which was initiated by the Muslim Brotherhood and Qatar-Turkey-Pakistan (QTP) nexus as explained in the Disinfo Lab report *"Muslim Brotherhood Arrives in India".* [18]

PSF's Conflict Analytics Division @AmRaadPSF was the first PSF handle to promote the video of a Chinese bot account within a few minutes after the video was posted. [19]

A few minutes later, the video originally posted by the Chinese bot account was reposted by *@ZEUS_PSF* which describes itself as the Founder & Team Lead of Pakistan Strategic Forum (PSF). [20] This is where the Galwan Valley propaganda

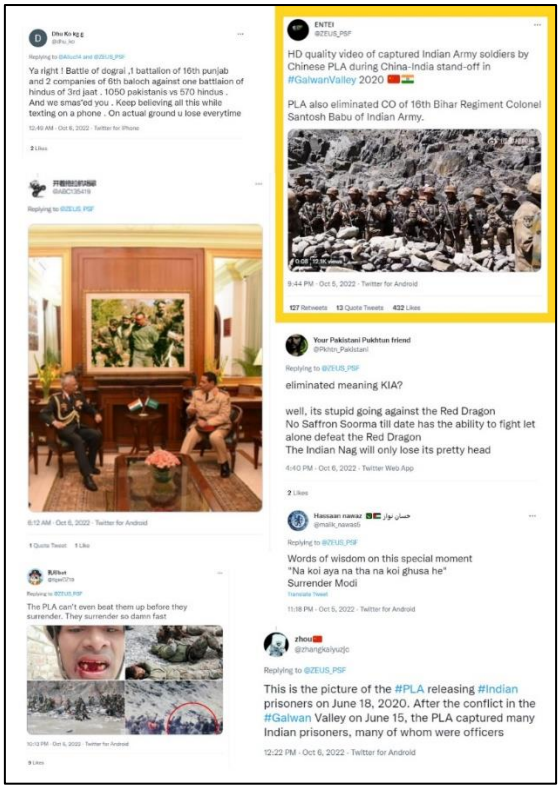
[13] https://twitter.com/Nickatgreat1220/status/1576131140771270656/retweets
[14] https://twitter.com/Nickatgreat1220/status/1576234894442700800/

[15] https://twitter.com/kt396/status/1577689301907034112
[16] https://pakstrategic.com/about-us/
[17] https://www.slideshare.net/AanisKamal/aanis-kamal-final-cv
[18] https://thedisinfolab.org/muslim-brotherhood-arrives-in-india/
[19] https://twitter.com/AmRaadPSF/status/1577692230617387014
[20] https://twitter.com/ZEUS_PSF

shoots up and where the Chinese and Pakistani social media warriors met over a single objective. [21]

Propaganda video reposted by the PSF founder

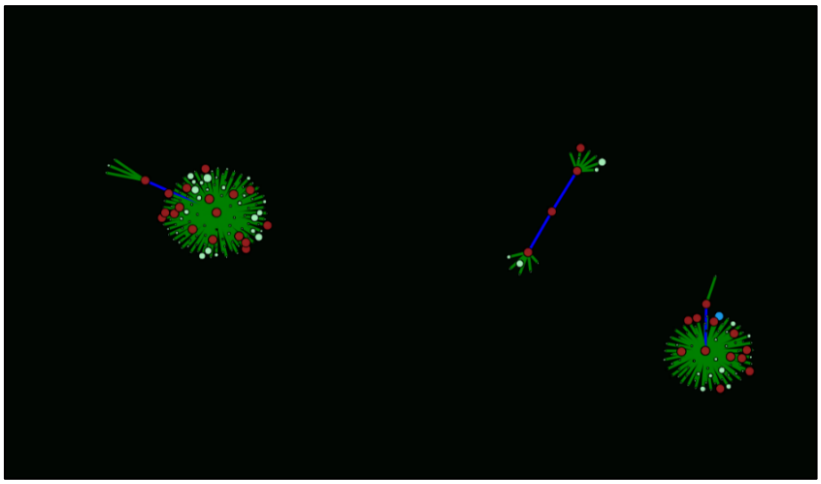
And this is where Pakistani social media picked the baton. @ZEUS_PSF's video helped disseminate Chinese propaganda into Pakistani social media.



A representative network shows how @ZEUS_PSF was the key handle in transitioning Chinese propaganda into Pakistan. An analysis of its network shows

[21] https://twitter.com/ZEUS_PSF/status/1577693687941066753

how his tweets were retweeted by hundreds of other Pakistani users to amplify the propaganda video originally seeded by a Chinese bot account.



Network of Pak accounts that amplified @ZEUS_PSF

And no Chinese propaganda is complete without the indulgence of its 'wolf-warrior' diplomats. Zhang Heqing, China's Cultural Counsellor at the Chinese embassy in Pakistan shared a video showing the heroics of Colonel Qi Fabao, the regimental commander of the People's Liberation Army Xinjiang military command, who was placed in Galwan during the clash with the Indian army in 2020. [22]

China has time and again politicized its propaganda to target nations. China hosted the 2022 Winter Olympics in February 2022. And to politicize the event the hosts continued to use the Galwan clashes in its anti-India narrative by selecting Col. Qi Fabao as the torch-bearer on the first day of its three-day tour in and near Beijing. [23] At that time, India denounced this politicization stunt by China and a diplomatic boycott of the event by not sending any Indian diplomat from its embassy to the opening and closing ceremonies. [24]

Most recently, the CCP invited Qi Fabao to the opening of the 20th National Congress of CCP on October 16 and also aired his video of the 2020 Galwan clash in the Great Hall of People. [25] And while the Indian and Chinese counterparts continue to engage in the de-escalation talks, China's apparent propaganda on Galwan is a part of CCP's achievements. Social media is among the key platform used by China and on occasion with its 'iron brother' Pakistan to rally joint propaganda when it comes to targeting a common enemy.

[22] https://twitter.com/zhang_heqing/status/1581537149991587840
[23] https://www.nytimes.com/2022/02/03/sports/olympics/china-torch-colonel-qi-fabao-india.html
[24] https://www.business-standard.com/article/current-affairs/beijing-olympics-indian-envoy-won-t-attend-opening-or-closing-ceremony-122020301577_1.html
[25] https://www.wionews.com/world/20th-cpc-national-congress-pla-galwan-commander-attended-opening-event-526039

Conclusion

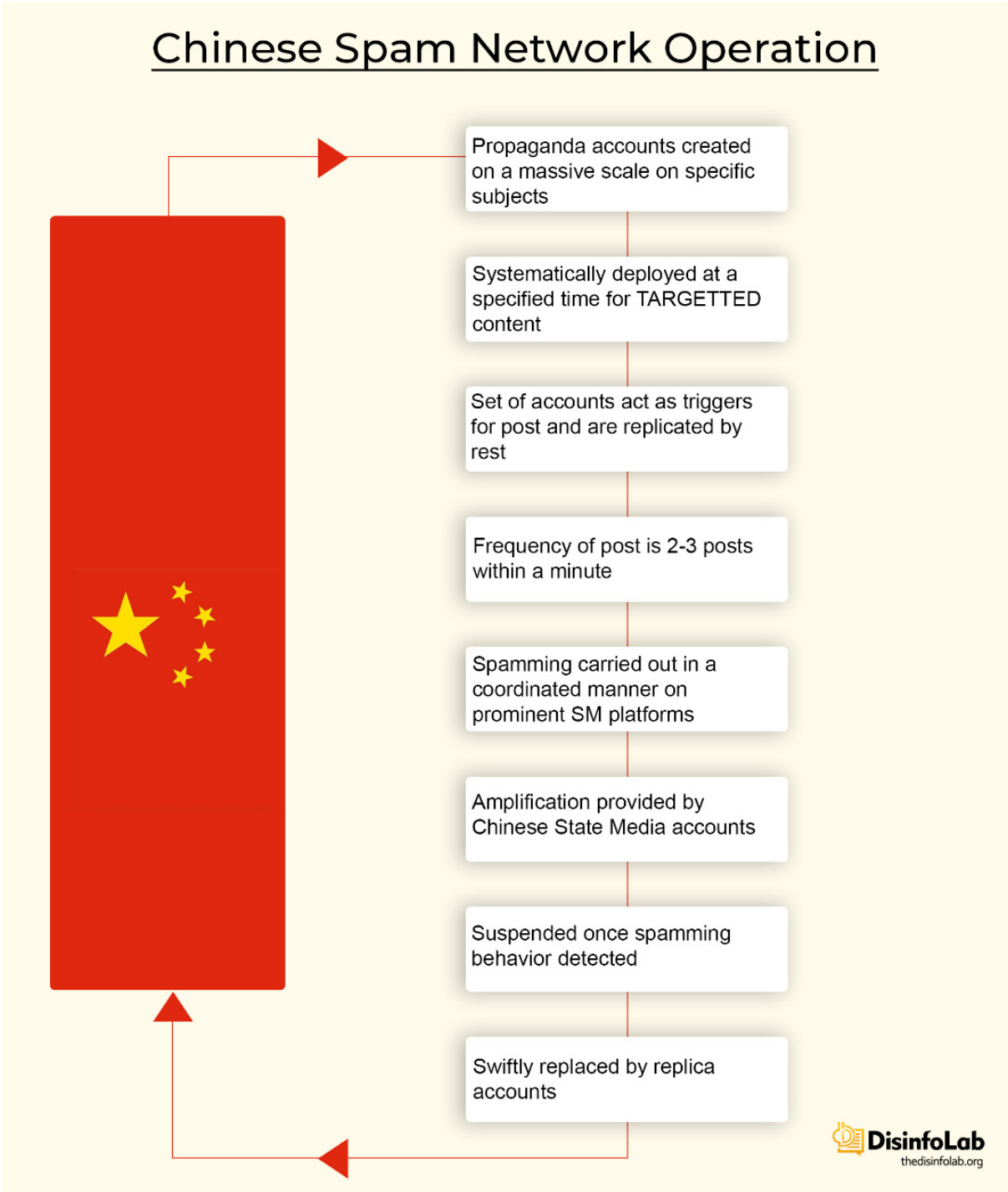
The famous decades-old term for "propaganda" or "publicity" in Chinese is defined as *"Xuanchuan",* which originally meant conveying information during the 3rd century. At present, Xuanchuan has become the keyword for propaganda in the People's Republic of China, which is carried out via the use of social media platforms.

And evidently, China seems to have mastered the social media operations of one of its kind. The 'spam network' cultivated as a part of these social media Ops tend to control the narrative on behalf of the People's Republic of China.

Internet censorship and surveillance remain tightly implemented in China has led to the ban of several social media platforms including Facebook, Instagram, Twitter, and Google among others. At the same time, Chinese social media operations rely on these very platforms for their existence, propaganda, and counter-propaganda.

Only that they are in large numbers. As noted, the Chinese spam networks are huge in the disposal that is deployed in many different ways as elaborated in our case studies. The spam network is so huge that even if many accounts are suspended, many such new accounts pop up to further the same propaganda.

Perhaps, these spam networks succeed in their pursuit in many instances of running their operations effectively. It is one of our efforts to shed light on such networks that flood social media that have become one of the key sources for information consumption as the internet continues to evolve.


Chinese Spam Network Operation
Propaganda accounts created on a massive scale on specific subjects
Systematically deployed at a specified time for TARGETTED content
Set of accounts act as triggers for post and are replicated by rest
Frequency of post is 2-3 posts within a minute
Spamming carried out in a coordinated manner on prominent SM platforms
Amplification provided by Chinese State Media accounts
Suspended once spamming behavior detected
Swiftly replaced by replica accounts
DisinfoLab
thedisinfolab.org