CHINA-LINKED INFLUENCE OPERATION ON TWITTER DETECTED ENGAGING WITH THE US PRESIDENTIAL ELECTION

PART 1: DETECTION REPORT
EXECUTIVE SUMMARY

This report describes a network of Twitter accounts with links to China, detected engaging in an influence operation targeting US politics and Covid-19 in the immediate run-up to the US Presidential election:

★ Seven days before the US presidential election, a network of over 500 accounts were detected engaging in co-ordinated inauthentic behaviour. Some accounts were operating in English language and others in Chinese, with matching personas.

★ Preliminary analysis revealed 54 of the active English language accounts were engaging with a range of topics related to US politics and the election within the last month. There is evidence of them increasing their activity in the run-up to the election.

★ These 54 accounts were forwarded to Twitter late-afternoon of 30/10/20 who suspended them all by the morning of 31/10/20. An additional 7 accounts that Twitter appear to have linked to the original set were also suspended.

★ The 54 were selected on the basis of possessing the potential to pose a risk to the integrity of the election and because we had higher confidence that they were engaging in inauthentic co-ordinated behaviour.

★ None of the accounts achieved much impact or engagement, and there is no evidence they have influenced events in the US based upon orthodox Twitter metrics. They may, however, have altered the content some users were exposed to by ‘gaming’ Twitter’s trending news algorithm.

★ In terms of messaging content, there was both anti-Trump and anti-Biden sentiments, but with a greater volume of the former. It is inferred that they were activated as a response to President Trump’s various claims that coronavirus was caused by China. There was a repeated focus upon Trump’s claim that disinfectant / bleach is a treatment for Covid-19.

★ The network was developed based on the likes of Chinese tweets that appeared to be artificially boosted. By mapping the recent liking behaviour of accounts involved with these tweets we were able to reveal the coordinated activity.

★ The network of accounts were only discovered because they had engaged in historic patterns of suspicious ‘liking’ behaviours in 2019 and February 2020. Looking only at their more recent behaviour, it is unlikely they would have been connected.

★ Only 1 pro-Trump account was identified in this network of 54 accounts. It is possible that accounts with a more pro-Trump political stance, run by the same or similar operators, exist but have not been picked up using the detection methodology described in the report.

★ Several signature tactics were being used by the accounts of interest. First, a lot of their activity involved selectively liking or reposting mainstream media articles aligned with the politically partisan stance they were adopting (ie. anti-Trump or pro-Biden). This enabled them to engage in activity without having to ensure their English was of a good standard. There are some examples of them trying to author original content and the written English is almost non-sensical.

★ More intriguingly, the reposting tactic may be designed to avoid platform detection algorithms that may focus more upon original messages. We have observed similar behaviour on Facebook, where disinformation is increasingly being inserted into comments to posts, rather than the posts themselves.

★ Another tactic involved a clear division of labour between accounts in the network functioning as ‘authors’ and ‘amplifiers’. The smaller number of authoring accounts were responsible for posting new content. They were boosted by a larger number of ‘amplifier’ accounts acting in co-ordination with the ‘primes’.
Many of the accounts were not especially sophisticated in terms of the deception employed. For example, a number had female account names, but males pictured in the biography. That said, they were active and had not been detected by Twitter.

There was a significant spike in account creation dates on two days in May 2018 and in April 2019. It is plausible that many of the accounts were purchased by the operators from a third-party supplier.

Using the behavioural signals that identified the initial set of 54 accounts that were validated by Twitter’s intervention, further investigation highlighted hundreds of additional ‘live’ accounts still active at the time of writing.

These accounts have continued to target US politics post-election, as well as a number of other topics of geopolitical interest to China, such as Taiwan and Hong Kong.

It is worth noting that Twitter is not legally available domestically within China, and as such, even though they are operating in Chinese language, they are targeting other audiences.

Below are two messages sent by ‘live’ accounts on 6th and 7th November (ie after the US voting had concluded) including potential vote-rigging and systemic racism claims, at a moment of particular uncertainty about the election outcome:

This second network of accounts are also observed engaging with Covid-19 narratives, especially seeking to cast doubt on claims that link the origins of the virus to a Chinese source, and networked targeted harassment of individual Western journalists responsible for stories perceived as degrading China’s reputation.

We suggest that on occasions, the Chinese accounts may have been paying external bot-farms to boost their messaging.

Based upon the open-source signals currently available to us, it is not possible to be more precise in terms of attribution and whether the activity described is linked to the Chinese state or not. However, this is considered plausible given the combination of behaviours and content discovered by the analysis. As such, throughout the report we refer to the network as ‘China linked’.
Seven days prior to the US Presidential election, a network of several hundred accounts were detected by the OSCAR programme at Cardiff University, potentially engaging in inauthentic co-ordinated behaviour. Some accounts were presenting with ‘Western’ identities, operating in the English language. A second group were using Chinese. It is relevant that Twitter is not legally available to citizens living in China, and so it can be reasonably inferred that any content communicated via this platform is targeted at external audiences. There was evidence of increasing levels of activity over the past few weeks, albeit no indicators of successful interference or influence. As the timeline in Figure 1 below shows, the network had displayed several peaks in activity. First in late February 2020 and May 2020, as part of the ‘I am not a virus’ campaign responding to President Trump’s claims about the Chinese origins of Covid-19. This was followed by a much quieter period over the summer and almost complete inactivity in September. They then re-activated in October this year with increasing levels of activity heading towards the election.

Figure 1: Aggregate Activity of the Chinese Language Accounts of Interest (N=281)
The screenshots in Figure 2 provide illustrative examples of the kinds of material that the accounts were sharing and reposting extensively in May:

Figure 2: English language account messages from May 2020

An initial dataset of 54 of the active English language accounts was established and investigated. Having scraped the last 400 likes for all of them, it was found that they had been engaging with a range of topics related to US politics and the election within the last month. Because of the potential risks to election integrity, and reflecting a high degree of confidence by the OSCAR research team, these 54 accounts were forwarded to Twitter late-afternoon of 30/10/20 who then suspended them all by the morning of 31/10/20. An additional 7 accounts from our larger network were also suspended by Twitter, we presume because Twitter had additional signals of co-ordination.

We delayed reporting the above because it was the run-up to the election, and in order to limit the possibility of encouraging ‘perception hacks’ that over-state the scale and impacts of (dis)information operations. This reflects a concern that the typical strategy used by platforms of publicising their account take-downs has created a societal vulnerability to perception hacks. This has been on display in some of the reporting around the 2020 election.

The report is organised around two principal sections. In the first part, we describe what has been distilled about the initial dataset of 54 English language accounts, in terms of their profiles and behaviour patterns. Section 2 uses these findings to develop an overview of the larger second cohort of ‘live’ accounts.

The background to this investigation commenced with research being conducted into a dataset of accounts released by Twitter in May 2020 comprising a large number of Chinese propaganda accounts. Analysis of this dataset suggested that these accounts had moved away from retweeting and were instead mainly ‘liking’ and commenting as their principal forms of interaction. The tweet by the account displayed in Figure 3 sent on 10th July 2019 was used to ‘seed’ the collection of the network of accounts that are the focus of this report. This is the only original tweet that the account made, and it received 142 comments, most of them from accounts suspended from Twitter. It made 7 reply tweets but these do not have any likes or retweets, and the account only has six followers. This tweet appears to be part of a campaign of Chinese tweets targeting Li Yiping using pictures of statements in Chinese. This is in keeping with the actions taken by the removed Chinese accounts in Twitter’s May 2020 dataset.

Figure 3: The ‘Seed’ Account and its sole authored Tweet
SECTION 1: RAPID NETWORK MAPPING

The network of interest was derived by scraping the last 400 ‘likes’ of accounts that had all liked the above tweet. This revealed a pattern of behaviour whereby there were a series of accounts almost exclusively liking each other’s tweets. Figure 4 provides a representation of one small cluster of accounts that are connected on the basis of their ‘liking relationships’, probably all engaged in coordinated inauthentic activity.

Figure 4: Small Cluster Embedded Within Larger Network Based on Liking Relationships

All of these accounts were targeting Chinese users, with anti-Trump, anti-Hong Kong protests and anti-Taiwan messages. Examples are provided below.

Figure 5: Anti-Trump Messaging

Application of this methodology resulted in scraping data from approximately 20,000 accounts. Most of these are not of interest and were collateral collection. Using the community detection algorithm in Gephi, we mapped the connections between nodes based upon the number of times an account has liked tweets from others. This resulted in a total of 43 communities being identified, most of which were very small and not relevant to this analysis. As illustrated in the graph in Figure 6, there were 3 very large clusters and 1 smaller one that are of direct interest herein.
Figure 6: Full Network Map Using Gephi of Approximately 20,000 Accounts

The most suspicious section of this graph is the top left, which contains a tightly clustered set of accounts, as depicted in higher resolution in Figure 7. Consequently, this was where investigative effort was directed.
Figure 7: Map of Tightly Clustered, Highly Connected Accounts

One of the accounts featuring prominently in this cluster was @HalleGmpduay. Tweets from this account have been liked by at least 20 other accounts. This was intriguing given that @HalleGmpduay had no followers or followees. It had, however, received likes and comments for ‘quote tweeting’ the tweet in Figure 1. It had also quote tweeted an account suspended from Twitter (@zydj1123), which was responsible for one of the most shared links in the China dataset released by Twitter in May 2020.

Also of note, is that messages by @HalleGmpduay were originally in Chinese (see Figure 8), but have more recently switched to non-native English (Figure 9).

---

1 The imprecision here of saying ‘at least’ relates to how it is not possible to obtain a list of accounts that have liked a specific account, such as @HalleGmpduay. We can only scrape all the likes of a specified account. So in this case, 20 scraped accounts have liked at least 1 Halle tweet.
The tweet feature in Figure 9 led us to search for other suspicious accounts in the dataset tweeting the same CNN link, trying to relate it to the controversy generated by President Trump’s unsubstantiated claim that disinfectant might aid coronavirus symptoms. This uncovered a significant pattern in terms of the content of messages in the densely connected cluster.

★ PROFILING THE ACCOUNTS

Filtering the tweets that were liked by accounts in the network, 62 accounts were highlighted for initial investigation. 11 of these 62 had Chinese symbols for their display names. Of these accounts, 3 tweeted in only Chinese (this does not include sharing of English articles), 1 account tweeted only English, and the rest were bilingual.

Focusing in upon the English-language account names within this set:

- ★ 8 accounts had 8 numbers after their Twitter names (so-called ‘numbers accounts’ where Twitter appends 8 numbers after a name during the account creation process to create a unique username);
- ★ 11 accounts had four numbers after their name;
- ★ 6 accounts had recognisable dates within their name;
- ★ 12 accounts seemed to be a random combination of letters and numbers (9 of these had a username 15 characters long).

Interestingly, researching the account creation dates identified some clear patterns, with a major spike in accounts being established in May 2018.
Several other identifying features were illuminated by the profiling exercise:

- **58%** of accounts did not have a bio. Of those that did, **13%** were written in Chinese language.
- **27%** of accounts included location data: 11 claimed to be in the US; 3 were in Chinese language and from ‘Mars’; ‘Singapore’; and ‘Not seeking the most educated but seeking the least serious’ respectively.
- Most accounts displayed a moderate, but not high level of activity.

In addition to the basic profiling work, an initial review was conducted of the contents being communicated. This identified a preponderance of anti-Trump messages, supplemented with anti-Biden and negative sentiments about the US more generally. There is a suggestion that the network’s activity was focused, in part, upon providing a reaction to President Trump’s allegation that Covid-19 originated in China. It was further evident that the accounts had seen a growth in their activity. Because of the potential risks to election integrity and reflecting a high degree of confidence by the analytic team, 54 accounts were forwarded to Twitter late-afternoon of 30/10/20 who suspended them all by the morning of 31/10/20. An additional 7 accounts that we infer Twitter had linked to the original set were also suspended.

**CONTENT ANALYSIS**

To develop further insights into how these accounts were being operationalised, manual thematic coding of 620 tweets was undertaken, sampled on the basis of the most recent 10 messages from each of the 62 original accounts. The purpose was to derive a picture of the key themes the accounts were collectively engaging with, and the relative frequency with which these themes were mentioned. An outline of the results is provided in Figure 11.

---

2 Not all 62 accounts were forwarded because, at the time, we were less confident in being able to connect them to the network.
The majority of themes were negative towards the US, Trump and Hong Kong. For example, 18 accounts were found to have communicated generally negative sentiments and opinions about President Trump, and ten explicitly commented negatively upon the disinfectant as a treatment for Covid-19 story. Six accounts expressed positive views about Vice-President Biden and his campaign, whilst seven engaged with positive messages about China, and five that the source of the virus was not China.

The second most frequent theme was associated with a link to a local news event in Minnesota about the bus services deteriorating because of coronavirus, which was heavily promoted by these accounts during a short period in May 2020. Examples of the key messages are provided in Figure 12.
At the current time, it is not clear what the purpose of this activity was. We hypothesise that it might have been the operators 'testing' their methodology to determine whether it would boost the visibility of the story via Twitter's algorithm. Similar examples of this behaviour have been found going back to April 2020, but it is entirely possible that it was occurring earlier in other networks. In this specific case, it was initiated by @HollyFayneman1, @2SDowlOJ1WvJdKZ and @apknar1 on the 12th May and by the 19th May, eleven suspicious accounts had tweeted this link, sometimes repeating the same tweet on consecutive days. These tweets received at least 130 likes from other accounts in the suspect network.

On the 8th of June another coordinated action took place promoting a CNN story about the President’s claim that disinfectant may be a treatment for coronavirus. This time four accounts were used, and they added comments with the link that contained slightly different narratives.

<table>
<thead>
<tr>
<th>Username</th>
<th>Tweet</th>
</tr>
</thead>
<tbody>
<tr>
<td>bemoxi2</td>
<td>terrible! This is really sad news! Why has nobody taught everyone how to use disinfectants? I really don’t want to see the tragedy happen again! us.cnn.com/2020/06/05/hea…</td>
</tr>
<tr>
<td>DjpuomrMoore</td>
<td>It’s hard to imagine that the President told us that we could drink disinfectant to prevent the virus; but now the CDC is telling us that it’s wrong to do that. We don’t know whether we should trust the President or the CDC us.cnn.com/2020/06/05/hea…</td>
</tr>
<tr>
<td>GardinerQvsnliz</td>
<td>I’m about to be laughed to death. I’m really deceiving myself. Maybe they think they can deceive the virus by doing so. This act of contempt for the virus is really the sorrow of all mankind; Amenlus.cnn.com/2020/06/05/hea…</td>
</tr>
<tr>
<td>FgyxqorZia</td>
<td>Trump’s wrong behavior has caused our bodies to be in danger us.cnn.com/2020/06/05/hea…</td>
</tr>
</tbody>
</table>

*Figure 12: Boosting the Bus Story from May 2020*

*Figure 13: CNN Disinfectant Story Amplification*
The interpretation included in the tweet in Figure 13 above about not knowing ‘whether we should trust the President or the CDC’ seems to connote the essence of the ‘play’. It is not directly or overtly critical, but clearly insinuates that trust is an issue.

Significantly, whilst most of the Chinese language accounts were displaying fairly typical troll behaviour, the cluster created in May 2018 with western style usernames, were evidencing an escalation in behaviour, tweeting mainstream media news stories attacking Trump. They were also sharing the same stories across accounts in the same order, which was an indicator of their coordination. This peaked at the end of October. A wordcloud derived from the tweets they have liked is provided below, to give an overview of their focus and interests.

![Wordcloud of US focused content themes](image)

It is worth noting the personas adopted by the English language accounts were not especially sophisticated or convincing, but given their behavioural patterns, they did not necessarily need to be to function as intended. In Figure 15 are displayed the biographical details provided for 6 of the accounts. In each case, it is noted that the image is of a male, but the first name in the identity is female. This was not apparently detected by Twitter’s algorithm.

![Account Bio Examples, May 2018 Cluster](image)
Initially, these accounts were used by their operators to tweet and like Chinese propaganda content, especially in February relating to the ‘I am not a virus’ campaign. This was originally a grassroots campaign initiated by French Asians using the hashtag JeNeSuisPasUnVirus at the end of January. The Chinese operator accounts started their own operation with this theme in February. However, after February 2020 these accounts have all been repurposed to spread English language content. With this tactical shift, it doesn’t appear as though they are using the same ‘liking’ strategies as before. This is noteworthy because, in their English-language configuration we would not have detected or connected them. It is only because of their behaviour patterns back in 2019 that we can link them as part of a co-ordinated network.

At the time we scraped them, these accounts had authored an average of 315 tweets (Max 525, Min 92) and had liked an average of 348 (Max 1047, Min 54). Their most recent 20 tweets evidence that they have been repeatedly posting mainstream media stories critical of President Trump with the tweet text just comprising the headline of the story. This is a rapid way for an account to deliver its mission, whilst minimising the chances of giving itself away due to poor language and grammar content for non-native operators. As visualised in Figure 16, collectively these accounts had increased their activity across October.

Two messages especially catch the eye. First, @GainsfordZaira tweeted a Washington Post story and accidentally included Chinese characters:

*Live updates: A major coronavirus vaccine trial paused over 鈥됬explained illness鈥* https://t.co/G1vchytBju

And @AaliyahColkins, retweeted a post from conservative commentator Buck Sexton:

*RT @BuckSexton: These “mostly peaceful protestors” sure do operate with the rehearsed tactics and cohesive maneuver of a domestic terroris…*

Overall, news stories from CNN and the Washington Post were the favoured outlets reposted by the Chinese operators in this network to develop their critical perspective on Trump. Table 1 shows where the 6 accounts highlighted above, sourced their material from.
Table 1: Media sources that were boosted

<table>
<thead>
<tr>
<th>Site</th>
<th>AaliyahColkins</th>
<th>ArianaGrove6</th>
<th>CynthiaMerewor1</th>
<th>FoljambeMontana</th>
<th>GainsfordZaira</th>
<th>HollyFayneman1</th>
</tr>
</thead>
<tbody>
<tr>
<td>edition.cnn.com</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>washingtonpost.com</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>bbc.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>nytimes.com</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>usatoday.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>npr.org</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>nbcnews.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>forbes.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>theguardian.com</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>cbsnews.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>politico.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>statnews.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>shawneemissionpost.com</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>cnn.com</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reuters.com</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ctvnews.ca</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>cnbc.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>apnews.com</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kstp.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>twitter.com</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scientificamerican.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

From the contents of this table, it is possible to adduce a clear sense of how the accounts were being operated. They were boosting stories aligned with what appears to be their mission to degrade the reputation of President Trump and his policies, by amplifying domestic sources. At the time of scraping, 6 of these tweets had received 1 retweet and one tweet had received 1 like. This suggests the operators were not bothering to boost their tweets. Instead their goal may be to ‘boost’ news stories to influence Twitter’s trending news algorithm.

Most of the accounts had similar numbers for likes and tweets. Only seven of the 33 accounts with recorded likes had more tweets than likes, and even then, the numbers were relatively similar. However, there were three accounts identified where the number of tweets and likes were very different. The inference we draw from this is that within the network as a whole there was a clear division of labour. A few accounts functioned as ‘primes’, supported by a larger number of ‘amplifiers’

Seven accounts performed one action exclusively (5 only reposted; one only sent replies; and a further one engaged solely in retweeting).
SECTION 2:
THE ‘LIVE’ LARGER NETWORK

Having flagged 54 of the accounts to Twitter with the result that they were rapidly suspended, we had a degree of confidence that the indicators listed in the preceding section were providing valid ‘signals’ of non-organic coordination and behaviour. Consequently, we applied a similar methodology to the remaining 532 accounts that, at the time of writing, were still ‘live’ and active. The results of this are outlined in this section of the report.

The graph below shows the liking activity of the accounts that we scraped that contribute to our most suspicious cluster. We tried to scrape the last 400 likes of 248 accounts and managed to retrieve 44,373 likes. This process will bias the graph in favour of dates closer to the scraping date, however only 54 accounts had over 400 likes. Of particular interest is the gap in activity between the end of October 2019 and January 1st 2020.

Figure 17: Timeline of Likes

Updating the full network graph in Figure 6, the ones sent to Twitter are highlighted in red, and other accounts they suspended are in green. Blue nodes have been scraped and pink nodes have not. The size of the node is based on how many accounts have liked tweets from that account. As can be seen, the majority of the US nodes were tightly clustered near the Chinese accounts, although some were halfway towards the liberal cluster in the bottom left corner and one was near the conservative cluster in the top right.
In an effort to understand the extent of the similarities between the initial set of accounts and the remainder of the suspicious cluster (N=532), the 20 most recent tweets from these 532 accounts were processed using analytics tools embedded within our bespoke Sentinel system.
Consistent with the earlier findings, this highlighted some suspicious account creation dates:

As visualised in Figure 19, there were clear surges in establishing new accounts. For example, on the 1st April 2019 twelve accounts were created between 2:11am and 3.11am, all with Cyrillic display names and their locations set to cities in Russia. Each username comprised 15 letters and digits.

Isolating a number of dates and looking in more detail at the timelines for account creation on each day highlights where they were created within minutes or even seconds of each other, particularly overnight between the 5th and 6th of April.

Attending to the timing of when accounts were established enabled the identification of several more suspicious accounts that weren’t obviously connected to the network from their liking behaviour alone. One plausible explanation for the temporal patterns observed, is that the accounts were purchased from an external supplier.
Analysing the content of the 532 accounts and their 20 most recent tweets was based upon several rapid sense-making tools integrated within Sentinel. Some key summary findings of most mentioned users and hashtags are provided in Figure 21.

Dissident Li YiPing was the main target for these accounts, being mentioned over 7 times more frequently than the second placed Twitter user. More interesting for our purposes here, however, are the hashtags mentioned by the accounts. For these collectively convey the operators’ clear interest in US and Taiwanese politics.

FlexiTerm\(^3\) analysis of the text content of tweets again highlights the Minnesota Bus campaign, as well as the large number of references made to Joe Biden. Qualitative dip-sampling suggests these references are more positive than those mentioning Trump.

Emoji analysis shows the second most popular emoji after the PRC flag is the rainbow usually used to denote LGBTQ support.

---

\(^3\) FlexiTerm is an open-source text analysis tool that identifies noun phrases within formal and informal texts, taking into consideration the main sources of term variation (such as acronyms) to provide robust aggregations of these terms.
More detailed investigation of the accounts displaying this flag seems to indicate that there is a sub-network of Chinese accounts seeking to present with an ‘LGBT identity’, retweeting anti-Trump stories primarily in Chinese. A selection of their messages are provided below.

Figure 24: Selection of Messages in Chinese

Figure 25 reproduces a message posted on 6th November, demonstrating how the ‘live’ accounts have been continuing their activity post-election where the result remained uncertain, amplifying claims that there were irregularities in the vote count.

Chuan Jianguo rushed to sue Sleepy Joe, but it was too late. Sleepy Joe was absolutely cheating, and the votes could not be seen at all. You see, the parcels counted are all SF Express sent from mainland China.

Figure 25: Example of post-election tweets amplifying uncertainty.
28% of the 532 accounts were set up as English language in their Twitter profile. However only 25% of the set’s tweets were in English.

![Comparative Language Distribution](image)

**Figure 26: Comparative Language Distribution**

Extending and elaborating this analysis, looking at both the users retweeted and the domains shared by the accounts overall, evidences a heavy Chinese influence, with state media accounts People’s Daily and CGTN retweeted, and Duowei News and Creaders being shared repeatedly.

![Users and Domains Shared](image)

**Figure 27: Users and Domains Shared**

Consistent with the previous findings about boosting Western media sourced content, further examples of these tactics were identified, including the Reuters story in Figure 28. This operation started on the 6th June, and was led by five western style accounts, supported by around 60 ‘boosting’ accounts. @SharkChili14 started the operation at 6.25am and Nathan Lee finished it at 6.58. There are far left narratives promoted in these tweets, such as the cops are the biggest gang in the world and that they cannot be reformed and must be destroyed.
Figure 28: Boosting a US Media Story About Policing

An example of one of the ‘booster’ accounts engaged in this operation is https://twitter.com/hailan666666. Set up in January 2019 with a Chinese character as its display name, it has made 46 tweets starting in March 2019. It started posting quotes in Chinese, but retweeted pro-China, anti-HK protest statements. In February 2020, it started posting in Chinese for the ‘I am not a virus’ campaign that we have seen many other Chinese accounts involved in. Its next original tweet came in October 2020 and between then and November 2nd it has posted inspirational English language quotes. The ‘inspirational quote’ activity is a documented behaviour of Chinese accounts and Internet Research Agency accounts, based upon evidence from previous Twitter dataset releases.

A new network graph below shows that the only likes the majority of these ‘booster’ accounts had in common were the 5 accounts above.

Figure 29: High Resolution View
In addition, the accounts in the top right-hand cluster of Figure 29, were responsible for pumping out anti-Trump memes and anti-trump tweets in Chinese between March and August 2020 (see Figure 30).

A more recent operation, utilising a similar tactical repertoire, was carried out against one of the authors of a New York Times article critical of the relationship between the World Health Organisation and China. Again, there appears to be a few main accounts tweeting about this in non-native English and receiving a disproportionate number of likes:
However, unlike the previous operation there does not appear to be a large number of closely associated ‘boosting’ accounts. The boosting seems to be coming from a different cluster, that was not captured in our original network map. These accounts appear to be under the direction and control of an outside actor, rather than the Chinese operators. The densely linked cluster below (Figure 32) is primarily made up from scraping 64 ‘seed’ accounts that had liked statuses related to this New York Times story.
Figure 32: Dense Cluster of Boosting Accounts Outside of Original Network
This cluster appears to be made up of accounts like these from the Philippines:

Figure 33: Examples of ‘booster’ accounts

The accounts in the center of this cluster most benefitting from these likes are usually verified accounts with tens or hundreds of thousands of followers. The two accounts who have received the most likes are the verified account of a Turkish mayor @Alinuraktas70 who was liked by 58 different accounts, and an unverified journalist from Turkey @medyaadami who was liked by 61 different accounts. This journalist appears to be spreading conspiracies relating to the Armenia conflict, such as:

Figure 34: Tweets Relating to the Nagorno-Karabakh Conflict

The intriguing implication here is that for this operation, the Chinese operators did not use their own accounts to boost their propaganda, but rather paid a bot farm to amplify it for them. This could make it more difficult to detect these types of operations in the future.
CONCLUSION

Overall, the China-linked network described appears to have achieved little in terms of meaningful impact and influence, as assessed by the orthodox metrics of retweets, interactions and followers. This relates both to the US presidential election and more generally. That said, there was clear evidence of an interest in the elections and related themes such as the management and origins of Covid-19. Also, it may be the case that the network has influenced the content displayed to some Twitter users. This is on the grounds that, when we tested where the New York Times news story appeared in the news feeds of the lead researcher for this report, who had been looking intensively at the accounts, it was placed as the 11th story. However, for other team members who had not been researching these accounts, the same story was ranked in the mid-20s.

Taken as a whole, many of the accounts, in terms of their presentation and messaging, were relatively unsophisticated. To a degree, this was compensated for by their deployment in a co-ordinated fashion, with a clear division of labour between authoring accounts and their supporting amplifiers. A key focus of the analysis has been distilling a number of key tactics and techniques operationalised by the network. Of particular note is a repeated pattern of behaviour of liking and/or re-posting mainstream media articles coherent with the ideological standpoint the account is adopting. Significantly, this signals a ‘full spectrum media’ strategy, wherein it is the interactions between media stories and social media accounts boosting and amplifying them, that needs to be the locus of analytic attention.

One benefit of a tactical focus on boosting, is that it does not require a high standard of English language proficiency. We also infer this tactic may be being used to try and circumvent the platform detection algorithms for co-ordinated inauthentic behaviour, where accounts may be more likely to be picked up if they are authoring original content. Similar patterns have recently been seen on Facebook, where disinformation content is increasingly being inserted into comments, rather than in a post initiating a thread.

It seems plausible that these avoidance measures are at least partially effective. After all, the detection of the network can be traced back to materials released by Twitter in respect of interventions conducted earlier in the year. It is thus somewhat surprising that Twitter did not identify this link themselves. The errors associated with the accounts are obvious to a human analyst, but appear sufficient to avoid automated detection methods. We would flag here the mixing the genders of account user images and names, and the fact that English language tweets were consistently being liked by accounts that operate in an entirely different language. Time constraints dictate that this is very much a ‘first cut’ analysis, providing an overview and initial insights into a significant network of accounts. Related to which, at the current time, we are not clear on what some aspects of the accounts’ behaviours signal or mean. Work is ongoing to establish what more can be gleaned about their purpose, and operational tactics and techniques.
ABOUT OSCAR

Cardiff University’s OSCAR (Open Source Communications Analytics Research) programme is a large-scale international research effort to understand the causes and consequences of information, influence and interference operations and disinformation campaigns. Supported by a range of partner organisations and agencies, the aim is to develop a more scientific and evidence-based perspective on how and why disinformation works to influence public perceptions and agendas. Blending methodologies and ideas from across the social, behavioural and data sciences, our highly experienced team of analysts have applied a range of tools and techniques, including state-of-the-art A.I., to study disinformation during election campaigns, public health crises and terror attacks. Our work has involved intensive investigations in over 20 countries worldwide.

GET IN TOUCH.

crimeandsecurity@cardiff.ac.uk
@CrimeSecurityCU

www.cardiff.ac.uk/crime-security-research-institute