ANCIR iLab

# The anti-China trolls

How a cluster of accounts leveraged on past controversies to spread a narrative of unauthorised Chinese surveillance on Africa

**09 / 2020**

# The anti-China trolls

## TABLE OF CONTENTS

# Glossary

Detailed descriptions and explanations of terms and abbreviations relevant to this report are listed below. These descriptions and explanations serve to clarify the usage in our report and are not intended to to be authoritative.

| Abbreviation | Description |
|---|---|
| ANCIR | African Network of Centres for Investigative Reporting |
| AU | Africa Union |
| CfA | Code for Africa |
| CIB | Coordinated Inauthentic Behaviour |

# Executive Summary

How a cluster of accounts leveraged on past controversies to spread a narrative of unauthorised Chinese surveillance on Africa

A CfA investigation identified a coordinated Twitter anti-China campaign that leveraged on past incidents and controversies involving China to build a tale of a continent under constant, unauthorised digital surveillance.

The perpetrators of this campaign leveraged on past controversies and published articles to build their narratives. One of the prominent narratives, that of the African Union's headquarters having been bugged by China, was based on a 2018 report by French newspaper Le Monde, which alleged that China had financed the construction of this building to enable them to spy on the AU. Both China and the AU dismissed this report, with the AU renewing its partnership with Huawei, a Chinese technology firm that supplied the building's computers, in 2019. Another narrative, of China led cyber-security attacks, was based on a 2014 incident in which 77 Chinese nationals were arrested in Kenya on suspicion of running a cybercrime hub, allegedly capable of infiltrating the country's communications systems.

The first hashtag, #JichoPevuChina, which in this context translates to, an investigative look into China, trended on 20 August 2020, spread a narrative of a China-led data harvesting exercise across Africa. Three weeks later, on 11 September 2020, a sudden surge in posts under a pre-existing hashtag #ChinaIsWatching, also spread a narrative of a China-led data harvesting exercise. Both trends claimed that China's presence in Africa was a front for a large-scale spying operation.

From an initial 5,240 tweets under both hashtags, we analysed 3,161 tweets and the resulting 9,134 retweets. Although three weeks apart, the trends employed an identical strategy of coordinated sharing of identical infographics,  a number of which were repeated across the trends. The images, seemingly pooled from a common source, bore a manipulated version of Kenya's coat of arms and a warning that the country is under Chinese surveillance. Additionally, we identified a cluster of accounts that participated in both trends, both through tweets and retweets.

# The Authors

Code for Africa (CfA) is the continent's largest network of non-profit independent civic technology and open data laboratories, with teams of full-time technologists and analysts in 13 African countries. CfA's laboratories build digital democracy solutions that give citizens unfettered access to actionable information to improve citizens' ability to make informed decisions, and to strengthen civic engagement for improved public governance and accountability.

The African Network of Centres for Investigative Reporting (ANCIR) is a CfA initiative that brings together the continent's best investigative newsrooms, ranging from large traditional mainstream media to smaller specialist units. ANCIR member newsrooms investigate crooked politicians, organised crime and big business. The iLAB is ANCIR's in-house digital forensic team of data scientists and investigative specialists who spearhead investigations that individual newsrooms are unable to tackle on their own. This includes forensic analysis of suspected digital disinformation campaigns aimed at misleading citizens or triggering social discord or polarisation using hate speech or radicalisation or other techniques.

The iLAB subscribes to CfA's guiding principles:

1. **We show what's possible.** Digital democracy can be expensive. We seek to be a catalyst by lowering the political risk of experimentation by creating successful proofs-of-concept for liberating civic data, for building enabling technologies and for pioneering sustainable revenue models.  We also seek to lower the financial costs for technology experimentation by creating and managing 'shared' backbone civic technology and by availing resources for rapid innovation.
2. **We empower citizens.** Empowering citizens is central to our theory of change. Strong democracies rely on engaged citizens who have actionable information and easy-to-use channels for making their will known. We therefore work primarily with citizen organisations and civic watchdogs, including the media. We also support government and social enterprises to develop their capacity to meaningfully respond to citizens and to effectively collaborate with citizens.
3. **We are action oriented.** African societies are asymmetric. The balance of power rests with governments and corporate institutions, at the expense of citizens.  Citizens are treated as passive recipients of consultation or services. We seek to change this by focusing on actionable data and action-orientated tools that give 'agency' to citizens.
4. **We operate in public.** We promote openness in our work and in the work of our partners. All of our digital tools are open source and all our information is open data.  We actively encourage documentation, sharing, collaboration, and reuse of both our own tools, programmes, and processes, as well as those of partners.
5. **We help build ecosystems.** We actively marshal resources to support the growth of a pan-African ecosystem of civic technologists. Whenever possible we reuse existing tools, standards and platforms, encouraging integration and extension. We operate as a pan-African federation of organisations who are active members of a global community, leveraging each other's knowledge and resources, because all of our work is better if we are all connected.

This report was authored by the iLAB's East African team, consisting of investigative manager Allan Cheboi, data analyst Jean Githae, data technologist Robin Kiplangat and datavis designer Odhiambo Ouma . The report was edited by senior programme manager Amanda Strydom and deputy CEO Chris Roper, and approved for publication by CEO Justin Arenstein.

# The Context

For the last seven years, China's Belt and Road Initiative (BRI) has taken shape in different countries across Africa, Asia and Europe. This initiative, which seeks to connect China to these continents, has been described by the Chinese government as "a bid to enhance regional connectivity and embrace a brighter future". The "belt" in this case refers to overland transportation networks - roads and railways - while the "road" refers to sea routes. The BRI provides infrastructural development loans to participating countries, which for many countries in Africa with inadequate infrastructure, has been a welcome addition. Notable infrastructural projects in Eastern Africa include the Addis Ababa-Djibouti Railway in Ethiopia, the Mombasa-Nairobi Standard-Gauge Railway in Kenya and the Entebbe-Kampala Expressway in Uganda.

While this initiative has been popular in African countries, many advanced economies have sharply criticised the potential debt crisis that shall arise. According to data from the China Africa Research Initiative (CARI), China has lent Africa at least $10-billion each year since 2012. In 2017, African countries comprised half of the top 50 nations most indebted to China, as a percentage of GDP. Djibouti, the world's highest, stood at an astounding 75%.

Africa has also seen increased activity from China through an influx of Chinese migrants over the past two decades. At first, the migrants were intermediaries between local entrepreneurs and Chinese warehouses, enabling the entrepreneurs to import goods at low prices. However, some of the entrepreneurs have abandoned their intermediary role, choosing to trade directly with the customers. In 2019, Kenya's Business Daily reported an influx of Chinese traders in Gikomba Market, one of Nairobi's largest open-air markets. Following public outcry, Kenya's interior ministry reported that the traders were in the country illegally and ordered for their immediate deportation.

This incident was not the first time that Chinese migrants faced public outcry. In 2014, 77 Chinese nationals were arrested on suspicion of running a cybercrime centre, allegedly capable of infiltrating the country's communications system. It is against this backdrop that the perpetrators of the anti-China campaign set their narrative.

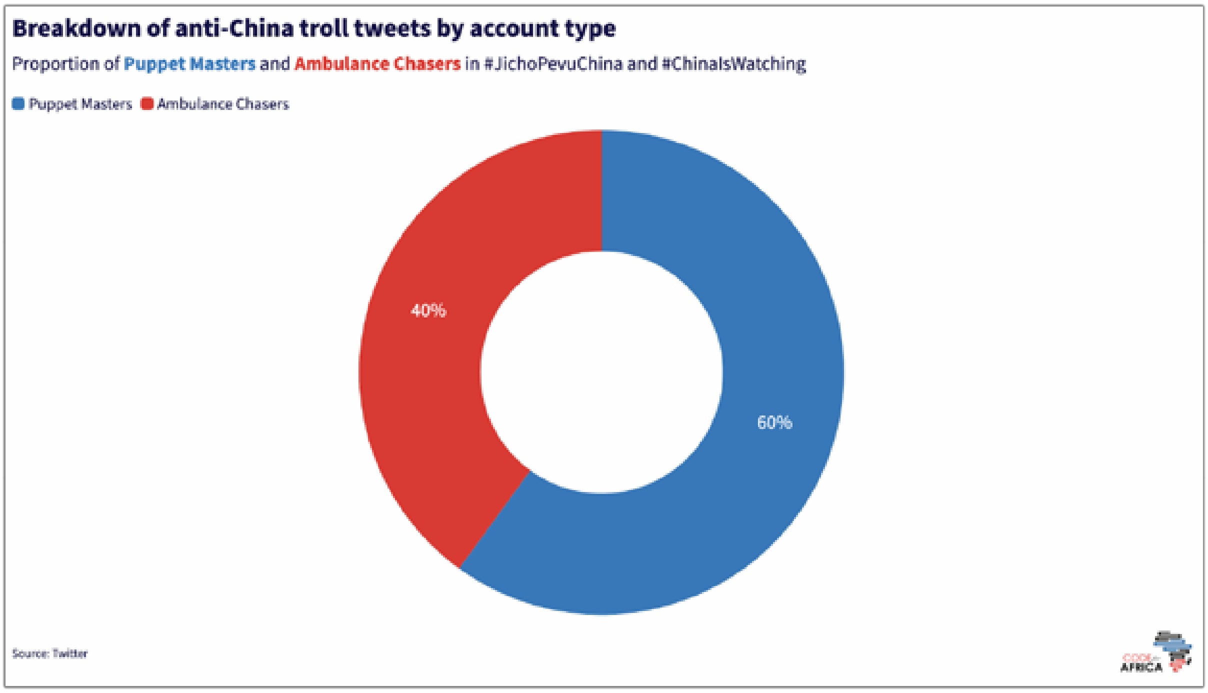
# The Network

## The ambulance chasers

In a previous investigation CfA observed a network of users who leverage on the popularity of the trending topics to market and promote goods and services. These accounts don't contribute to the narrative being shared within the trends and tend to follow these characteristics:

1. Tweeting with excessive, unrelated hashtags (usually the top trending hashtags for the day) in a single tweet or across multiple tweets;
2. They tend to drive traffic or attention from a conversation on Twitter to accounts, websites, products, services, or initiatives;
3. The tweets contain contact information such as phone numbers and email. Users are directed to either call, or send a message via sms and WhatsApp .

The network's assets interspersed their advertisement/ marketing posts with high volumes of hashtags, links to websites and contact information. CfA named this network "the ambulance chasers". Out of 5,240 tweets collected for the two anti-China hashtags, 2,079 were categorised as ambulance chasers, representing 40% of the tweets in the network. This behaviour has become an increasingly popular phenomenon observed in both legitimate and coordinated trends on Kenyan social media.


**Breakdown of anti-China troll tweets by account type**

Proportion of Puppet Masters and Ambulance Chasers in #JichoPevuChina and #ChinaIsWatching

Source: Twitter

Given that these tweets do not directly contribute to the narrative under investigation, we excluded them from our analysis. This kind of parasitic behaviour is corrosive to the discussions and narratives being conducted on social platforms and undermines civic discourse and digital democracy.

## The Puppet Masters

The puppet masters, who we define as the contributors and direct drivers of the anti-China narrative, were responsible for 3,161 tweets and 9,134 retweets in both hashtags. The tweets originated from 551 unique accounts while the retweets originated from 1,293 unique accounts. Additionally, we identified a cluster of 74 accounts who posted in both hashtags; 24 of which were responsible for the tweets and 50 of which were responsible for retweets. We also noted that the activities of this cluster of accounts accounted for 30% of all tweets and 42% of all the retweets across the two hashtags, despite the number of unique accounts from the network representing less than 6% of the total number of unique accounts.

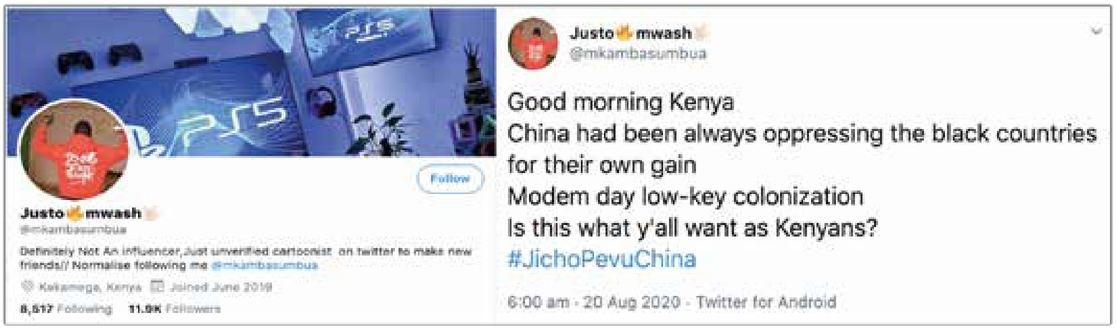
### Top 10 Twitter profiles with the most ineraction rates on the network : Most intractive Accounts

| Account | Number of Tweets | Account | Number of Retweets |
|---|---|---|---|
| addihuche | 82 | AddihUche | 235 |
| evelynmuoki | 61 | Kenyan_Bee | 171 |
| jmekaofficial | 49 | faith_ke2 | 162 |
| allannyash | 48 | Evelynmuoki | 159 |
| _techguru__ | 46 | Aryannkinyua | 124 |
| droffilcremone | 45 | Doktari_owori | 121 |
| brian_mogenii | 44 | skimaskmkonde | 113 |
| i___ambrad | 39 | iam_jaymoe | 108 |
| iamkuriah | 33 | TunoiAustin | 107 |
| baewakoo | 32 | MkenyaKe1 | 100 |

# Timeline Mapping

## JichoPevuChina

A tweet by user @mkambasumubua posted on 20 August 2020 initiated conversations under the hashtag #JichoPevuChina. This set the stage for a series of coordinated posts alleging that China was engaged in a massive data extraction exercise in Africa, through hacking into the AU's servers, bugging the AU's headquarters in Addis Ababa to monitor communications and spying on Africans through their mobile devices and computers. Notably, as at 14 October 2020, the account had changed its name and username to 'premierwriter01. essays. hw. assignment.' and @premierwriter01 respectively.

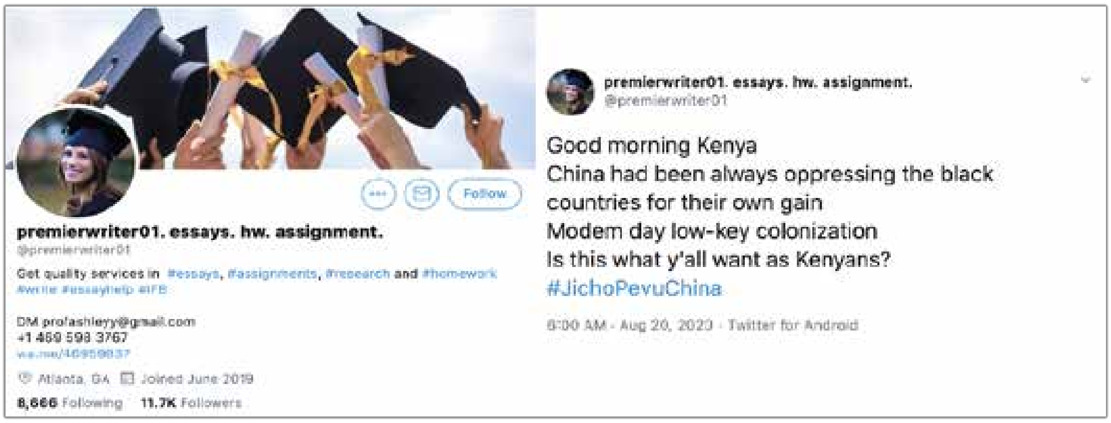


Justo ✌ mwash ✌
@mkambasumbua
Definitely Not An influencer,Just unverified cartoonist on twitter to make new friends// Normalise following me @mkambasumbua
Kakamega, Kenya Joined June 2019
8,517 Following 11.9K Followers

Justo ✌ mwash ✌
@mkambasumbua

Good morning Kenya
China had been always oppressing the black countries for their own gain
Modem day low-key colonization
Is this what y'all want as Kenyans?
#JichoPevuChina

6:00 am · 20 Aug 2020 · Twitter for Android



premierwriter01. essays. hw. assignment.
@premierwriter01
Get quality services in #essays, #assignments, #research and #homework #write #essayhelp #IFB

DM profashleyy@gmail.com
+1 469 598 3767
wa.me/46959837
Atlanta, GA Joined June 2019
8,666 Following 11.7K Followers

premierwriter01. essays. hw. assignment.
@premierwriter01

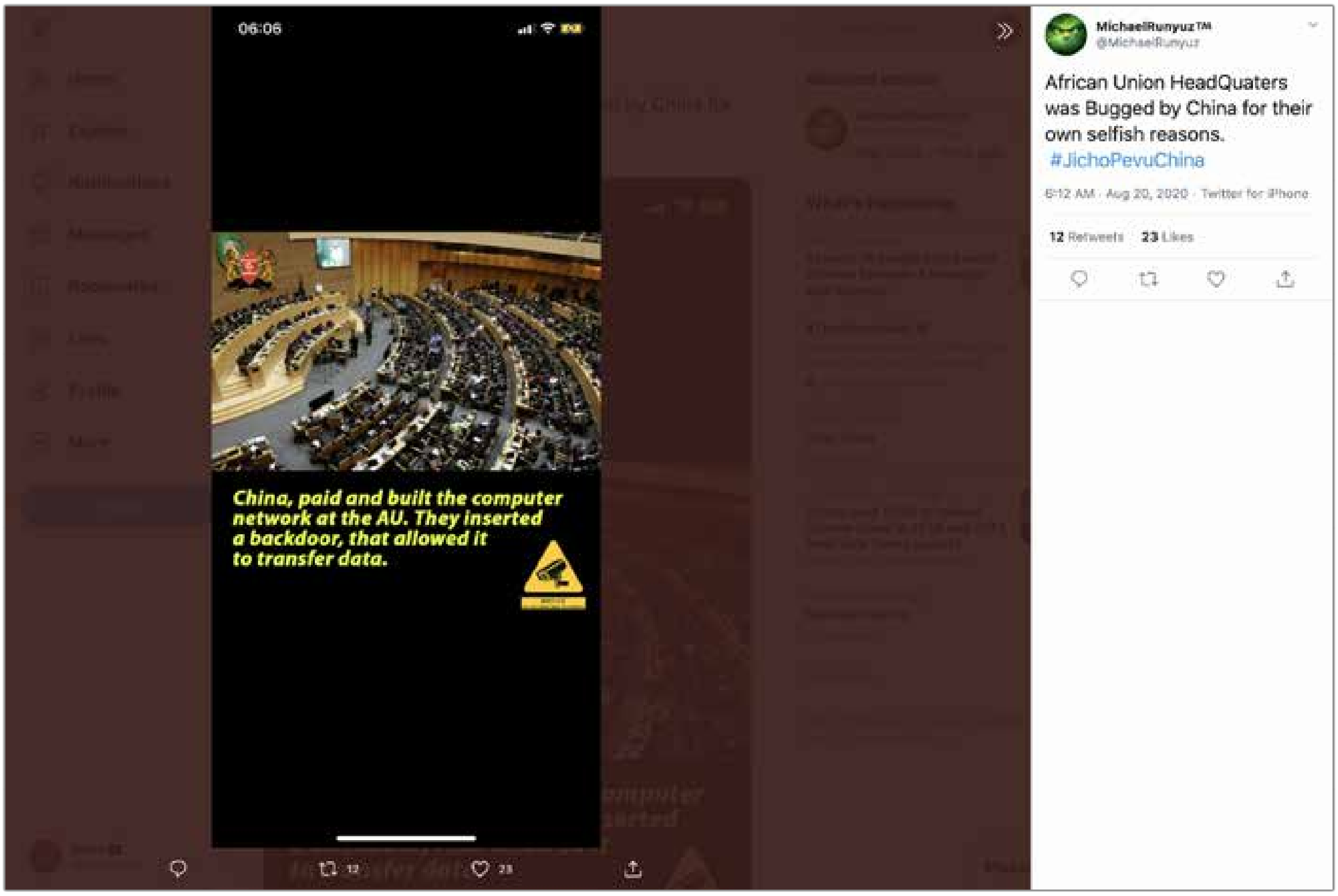
Good morning Kenya
China had been always oppressing the black countries for their own gain
Modem day low-key colonization
Is this what y'all want as Kenyans?
#JichoPevuChina

6:00 AM · Aug 20, 2020 · Twitter for Android

We further noted that the self-declared location of the account was Atlanta, Georgia and the account was created in June 2019.

A key characteristic of this campaign was the coordinated sharing of identical infographics, which spread the different narratives.

The first of these infographics, on the AU spying claim, was shared by @MichaelRunyuz. We observed that the image was a screenshot upload, rather than an upload of the image itself. This image was posted six more times by five different users over the next 90 minutes, suggesting that the images were pooled from a common source for coordinated dissemination.


06:06
China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.
12
23

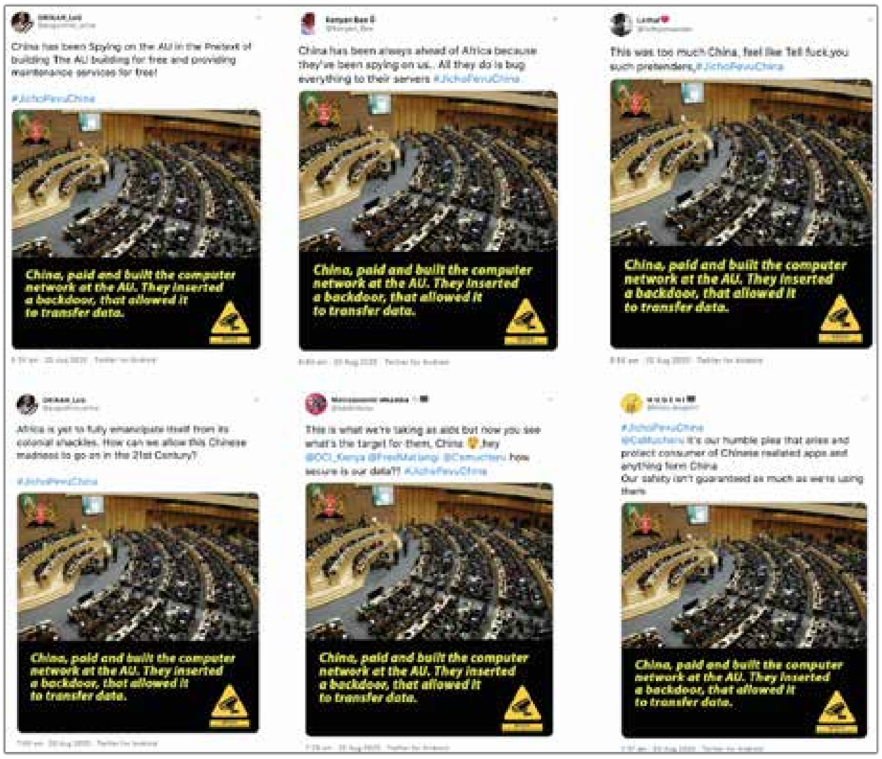
MichaelRunyuz™
@MichaelRunyuz

African Union HeadQuaters was Bugged by China for their own selfish reasons. #JichoPevuChina

6:12 AM · Aug 20, 2020 · Twitter for iPhone

12 Retweets 23 Likes

**Screengrab of @MichaelRunyuz's infographic, showing the time the screenshot was taken(Source: Twitter/CfA)**



China has been Spying on the AU in the Pretext of building The AU building for free and providing maintenance services for free!

#JichoPevuChina

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

China has been always ahead of Africa because they've been spying on us.. All they do is bug everything to their servers #JichoPevuChina

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

This was too much China, feel like Tell fuck you such pretenders,#JichoPevuChina

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

Africa is yet to fully emancipate itself from its colonial shackles. How can we allow this Chinese madness to go on in the 21st Century?

#JichoPevuChina

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

This is what we're taking as aids but now you see what's the target for them, China 🤔,hey @DCI_Kenya @FredMatiangi @Cmuchiru how secure is our data?? #JichoPevuChina

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

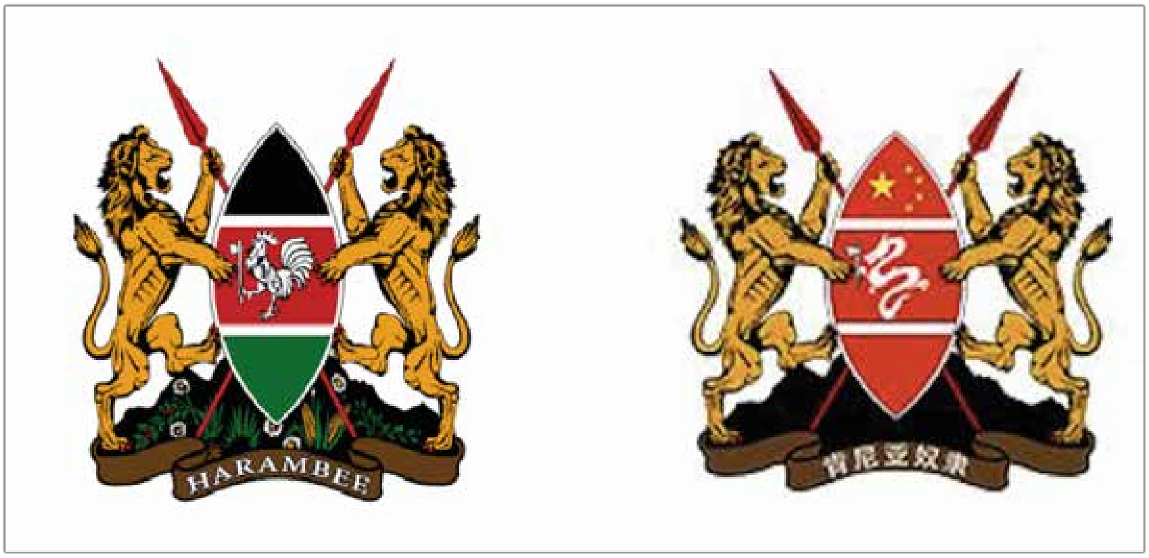
#JichoPevuChina
@CaMucheru It's our humble plea that aries and protect consumer of Chinese realated apps and anything form China
Our safety isn't guaranteed as much as we're using them

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

**Screengrabs of infographics claiming that China transfers data from the AU's computer networks (Source: Twitter/CfA)**

Over the course of this trend, more infographics were posted by different accounts, specifically in the first five hours of the trend. Each infographic contained a manipulated version of Kenya's coat of arms.

Kenya's coat of arms features a shield in the national colours of black, white, red and green, on which there is a cockerel holding an axe. The shield rests on a silhouette of Mount Kenya, which features Kenyan agricultural produce and is supported by a scroll inscribed 'Harambee', which means "pulling together" in Kiswahili. The manipulated version had the shield painted in the colours of the Chinese flag, replaced the cockerel with a snake, stripped the agricultural produce off the silhouette and replaced the phrase 'Harambee' with Chinese text



**Side by side comparison of the real and manipulated Kenya coat of arms**

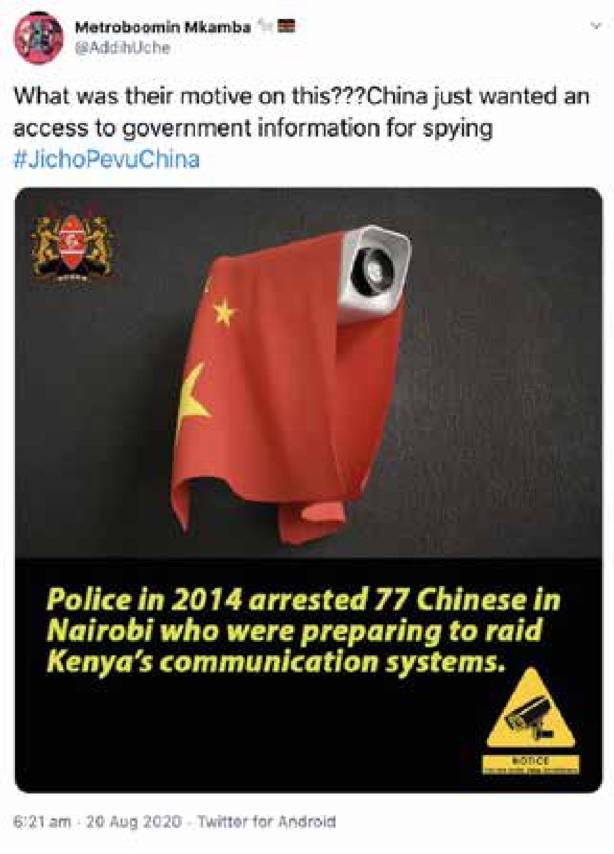
An analysis into the narratives spread using the infographics posted in the first five hours of the trend led us to the following reports and incidents:

1. 2014 cybersecurity incident involving Chinese nationals in Kenya: In 2014, 77 Chinese nationals were arrested on suspicion of running a cybercrime centre, allegedly capable of infiltrating the country's communications system. The systems mentioned in this incident were allegedly capable of infiltrating bank accounts, M-Pesa accounts and ATMs. M-Pesa is Kenya's leading mobile money transfer service, with an average of 24 million active customers a month.

   From this incident, we identified an infographic highlighting the arrest. This infographic, which was posted 13 times and retweeted 175 times, consisted of a CCTV camera draped in China's flag, possibly alluding to the alleged constant surveillance the country would have faced. A second infographic reported on the financial systems hacking capability of the cybercrime systems, and was posted six times and retweeted 30 times.

2. A 2018 claim that the AU's headquarters have been bugged by China: In 2018, an investigation by French newspaper Le Monde, alleged that China's financial contribution to the construction of the African Union's headquarters' was a front for China to spy on Africa. The report claimed that China infiltrated the computer systems and siphoned data between 2012 and 2017. This activity was discovered by the AU's technicians, who noted a peak in server activity between midnight and 2am. These claims were dismissed by the AU and China.

   From this report we identified an infographic reporting on the alleged backdoor data transfer from the AU's computer networks. This infographic was posted six times and retweeted 75 times. A second infographic, highlighting the alleged five-year timeline of the data transfer occurred between 2012 and 2017 was posted once and retweeted six times . A third infographic, which was posted twice and retweeted 21 times, claimed that the AU kept this information secret for a year after making this discovery.

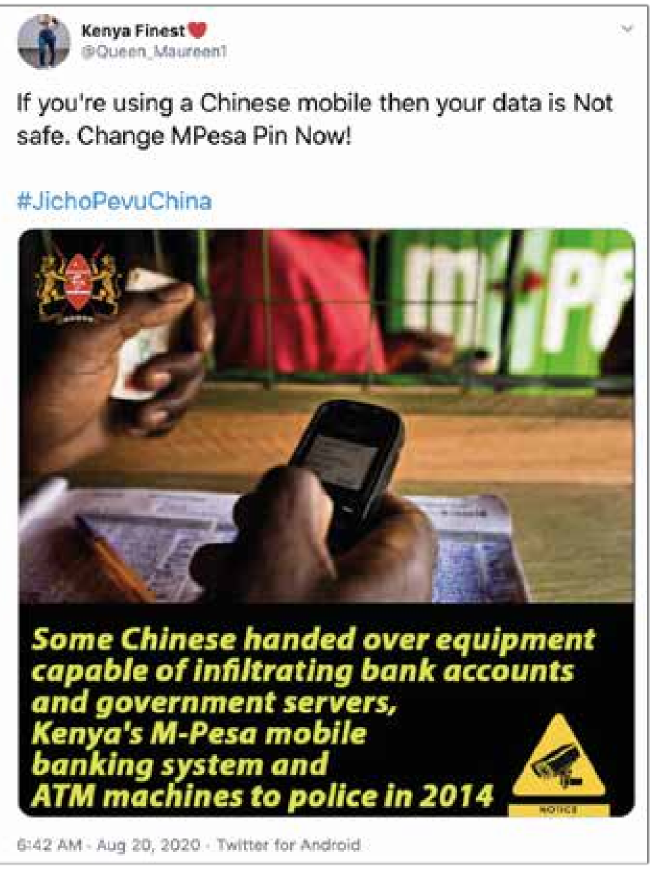


Metroboomin Mkamba
@AddihUche

What was their motive on this???China just wanted an access to government information for spying
#JichoPevuChina

Police in 2014 arrested 77 Chinese in Nairobi who were preparing to raid Kenya's communication systems.
NOTICE

6:21 am · 20 Aug 2020 · Twitter for Android



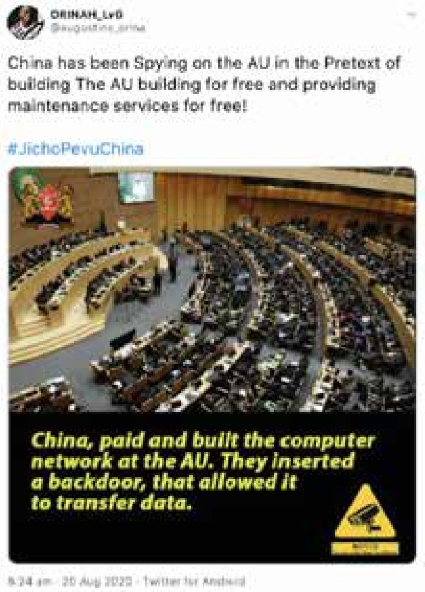
Kenya Finest❤️
@Queen_Maureen1

If you're using a Chinese mobile then your data is Not safe. Change MPesa Pin Now!

#JichoPevuChina

Some Chinese handed over equipment capable of infiltrating bank accounts and government servers, Kenya's M-Pesa mobile banking system and ATM machines to police in 2014
NOTICE

6:42 AM · Aug 20, 2020 · Twitter for Android



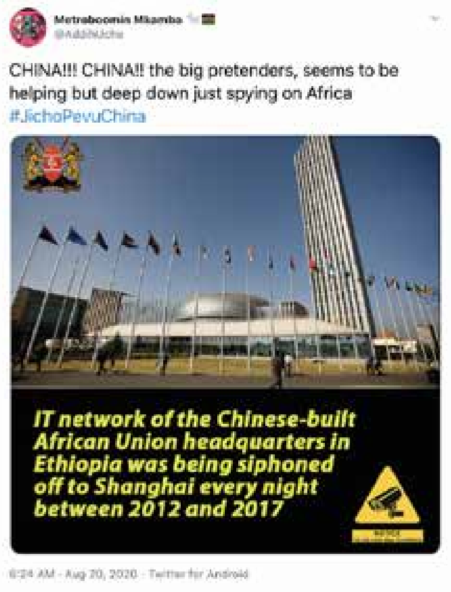
ORINAH_Lv6
@augustine_orina

China has been Spying on the AU in the Pretext of building The AU building for free and providing maintenance services for free!

#JichoPevuChina

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.
NOTICE

6:24 am · 20 Aug 2020 · Twitter for Android

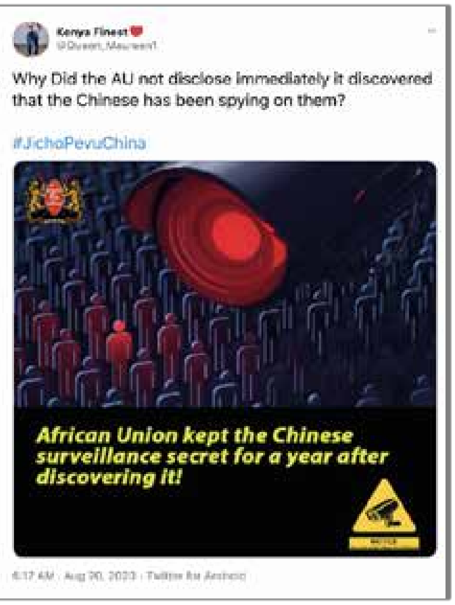


Metroboomin Mkamba
@AddihUche

CHINA!!! CHINA!! the big pretenders, seems to be helping but deep down just spying on Africa
#JichoPevuChina

IT network of the Chinese-built African Union headquarters in Ethiopia was being siphoned off to Shanghai every night between 2012 and 2017
NOTICE

6:24 AM · Aug 20, 2020 · Twitter for Android



Kenya Finest❤️
@Queen_Maureen1

Why Did the AU not disclose Immediately it discovered that the Chinese has been spying on them?

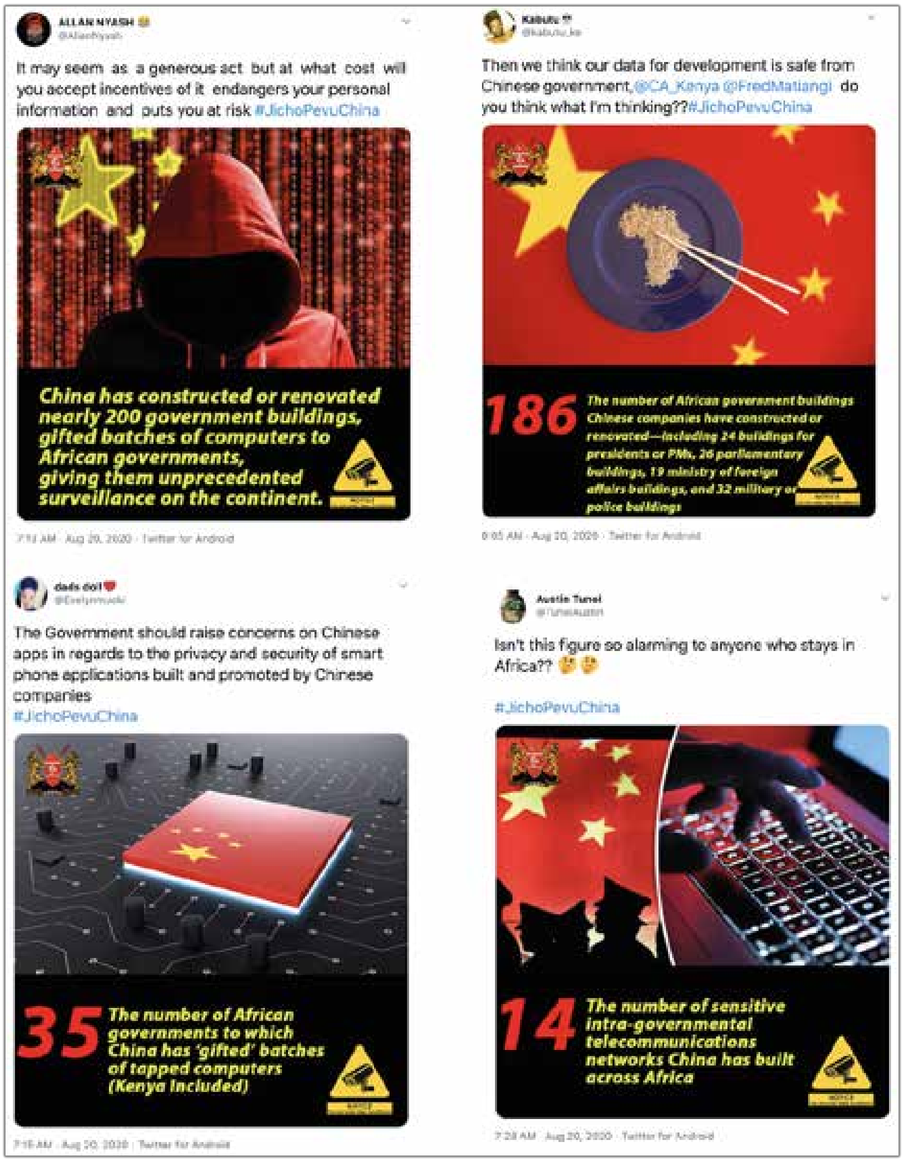
#JichoPevuChina

African Union kept the Chinese surveillance secret for a year after discovering it!
NOTICE

6:17 AM · Aug 20, 2020 · Twitter for Android

3. A 2020 report alleging that government buildings across Africa are a possible conduit for Chinese spying: This 2020 report by the Heritage Foundation highlights that Chinese companies have built at least 186 government buildings and at least 14 sensitive intra-governmental telecommunication networks. Chinese companies are legally obliged to help the Chinese Communist Party (CCP) to collect intelligence. The report also highlights that the Chinese government has donated office computers to at least 35 African governments, and suggests that the Chinese government bugged the devices. However, this report presents no factual evidence to support its claims.

   From this report, we identified an infographic highlighting that 200 African government buildings which China has constructed are under their surveillance. This was posted thrice and retweeted 24 times. A second infographic broke down the types of government buildings named in the report: parliamentary, foreign affairs and military offices. This was posted twice and retweeted 11 times. A third infographic, highlighting that 35 African countries which received computer donations are also under surveillance, was posted thrice and retweeted eight times. A final infographic, posted once and retweeted thrice, reported on the Chinese-built telecommunications networks.



ALLAN NYASH
@AllanNyash

It may seem as a generous act but at what cost will you accept incentives of it endangers your personal information and puts you at risk #JichoPevuChina

China has constructed or renovated nearly 200 government buildings, gifted batches of computers to African governments, giving them unprecedented surveillance on the continent.

7:13 AM · Aug 20, 2020 · Twitter for Android

Kabutu
@kabutu_ke

Then we think our data for development is safe from Chinese government,@CA_Kenya @FredMatiangi do you think what I'm thinking??#JichoPevuChina

186 The number of African government buildings Chinese companies have constructed or renovated—including 24 buildings for presidents or PMs, 26 parliamentary buildings, 19 ministry of foreign affairs buildings, and 32 military or police buildings

9:05 AM · Aug 20, 2020 · Twitter for Android

dads dol❤
@Evelynmuoki

The Government should raise concerns on Chinese apps in regards to the privacy and security of smart phone applications built and promoted by Chinese companies
#JichoPevuChina

35 The number of African governments to which China has 'gifted' batches of tapped computers (Kenya Included)

7:16 AM · Aug 20, 2020 · Twitter for Android

Austin Tunei
@TuneiAustin

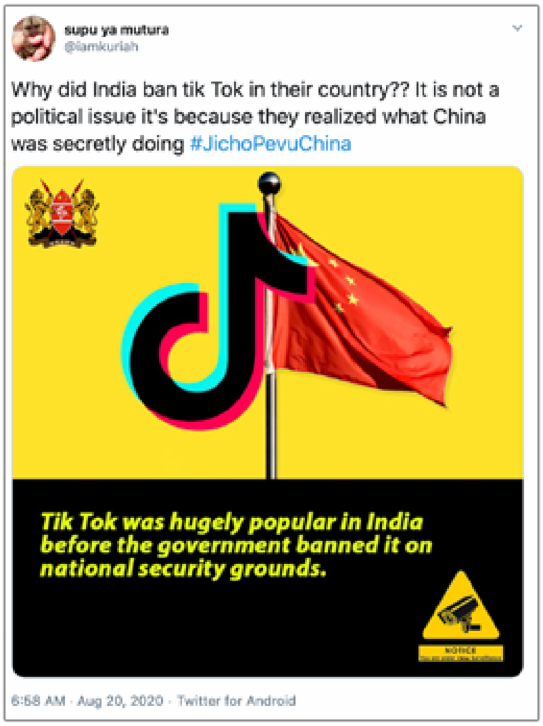
Isn't this figure so alarming to anyone who stays in Africa?? 🤔🤔

#JichoPevuChina

14 The number of sensitive intra-governmental telecommunications networks China has built across Africa

7:28 AM · Aug 20, 2020 · Twitter for Android

4. India’s 2020 TikTok ban: In June 2020 India banned TikTok, a popular video sharing app, and numerous other Chinese apps, over concerns that the apps were engaging in activities that threatened the national security and defence of India. We identified this information in an infographic which was posted six times and retweeted 89 times.



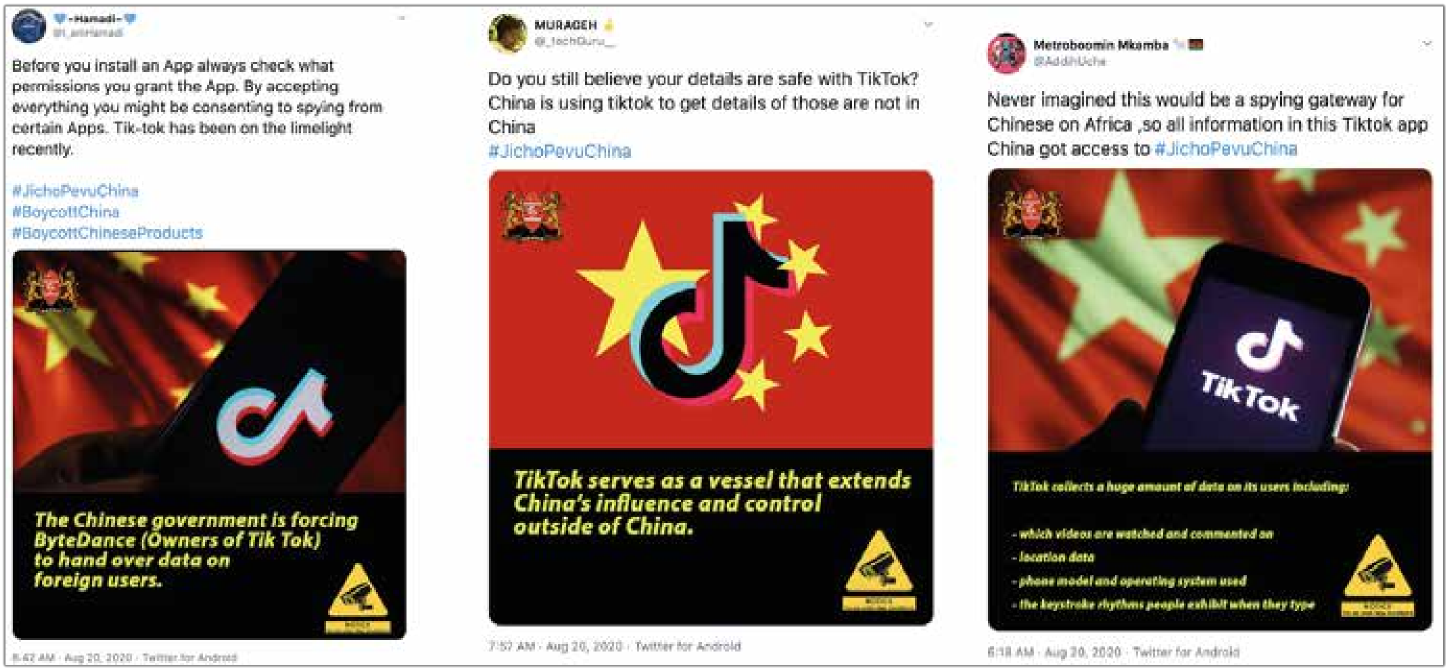
supu ya mutura
@iamkuriah

Why did India ban tik Tok in their country?? It is not a political issue it's because they realized what China was secretly doing #JichoPevuChina

Tik Tok was hugely popular in India before the government banned it on national security grounds.

6:58 AM · Aug 20, 2020 · Twitter for Android

Following on the TikTok narrative, we identified additional infographics which claimed that TikTok’s parent company, ByteDance, is mandated to hand over all data on foreign users to the Chinese government; TikTok collects different personal data points from users including location data, device data and keystroke rhythms; and that TikTok serves as a vessel for China’s influence abroad. These infographics were posted a total of 10 times and retweeted 62 times.



-Hamadi-
@i_amHamadi

Before you install an App always check what permissions you grant the App. By accepting everything you might be consenting to spying from certain Apps. Tik-tok has been on the limelight recently.

#JichoPevuChina
#BoycottChina
#BoycottChineseProducts

The Chinese government is forcing ByteDance (Owners of Tik Tok) to hand over data on foreign users.

8:42 AM · Aug 20, 2020 · Twitter for Android

MURAGEH
@_techGuru_

Do you still believe your details are safe with TikTok? China is using tiktok to get details of those are not in China
#JichoPevuChina

TikTok serves as a vessel that extends China’s influence and control outside of China.

7:57 AM · Aug 20, 2020 · Twitter for Android

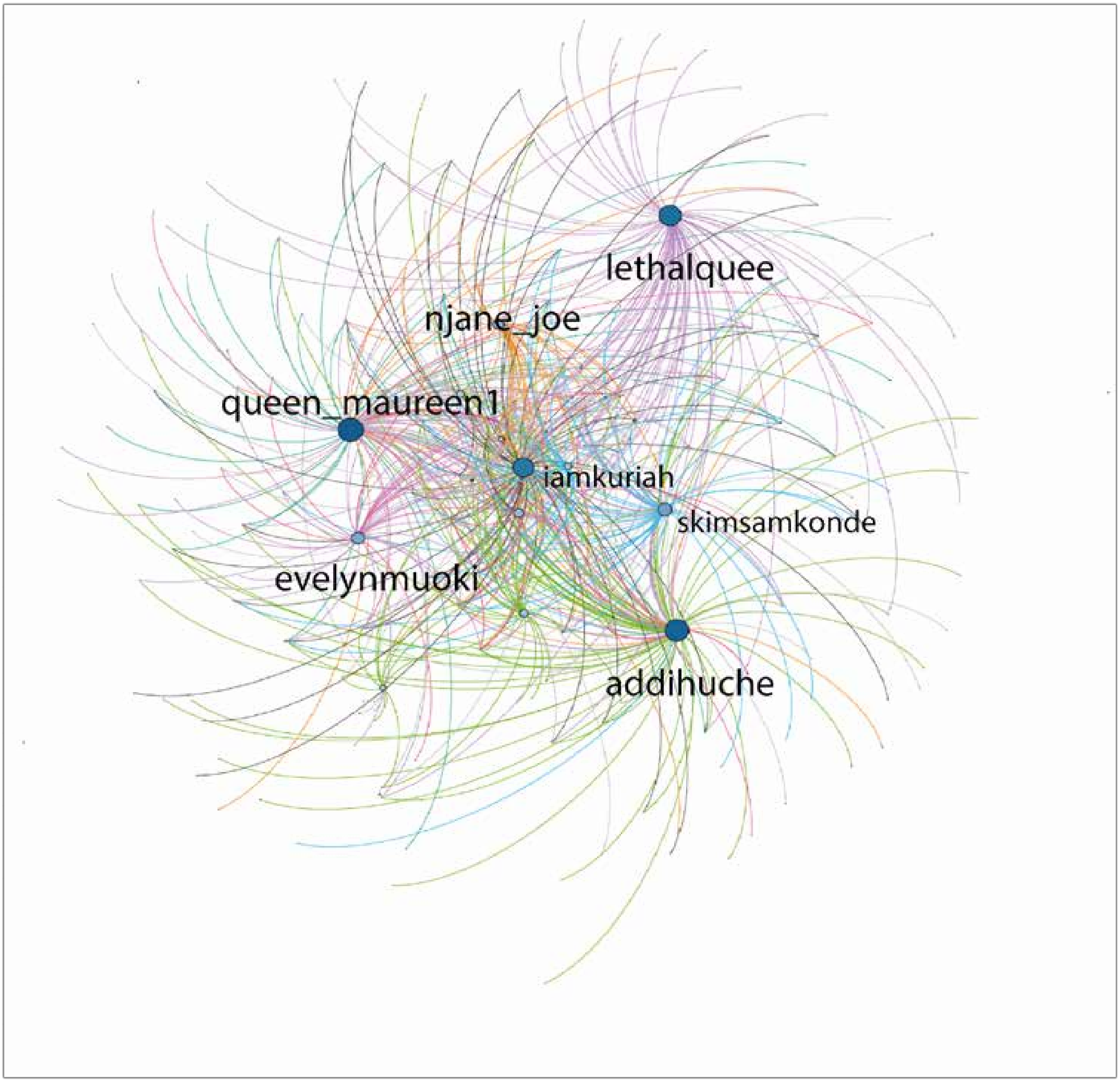
Metroboomin Mkamba
@AddihUche

Never imagined this would be a spying gateway for Chinese on Africa ,so all information in this Tiktok app China got access to #JichoPevuChina

TikTok
TikTok collects a huge amount of data on its users including:
- which videos are watched and commented on
- location data
- phone model and operating system used
- the keystroke rhythms people exhibit when they type

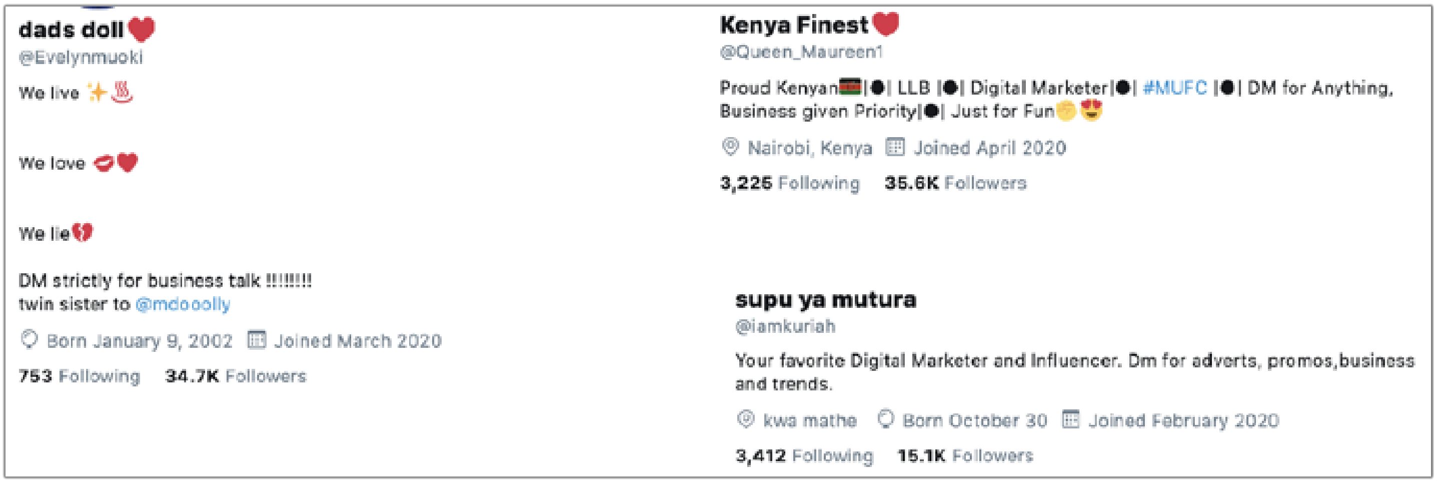
6:18 AM · Aug 20, 2020 · Twitter for Android

A network analysis of the accounts that posted and retweeted the infographics in the first five hours of the trend shows a cluster of accounts acting as key amplifiers of these infographics. The tweets came from @queen_maureen1, who posted eight different images.



**Network analysis of accounts sharing the infographics under #JichoPevuChina (Source: CfA via Gephi)**

An analysis of the key accounts in this network revealed that these accounts are probable online marketer accounts, simply hired to push a given trend. The profiles of queen_maureen1, evelynmuoki and iamkuriah describe them as digital marketers and influencers. These accounts, all created in 2020, all have at least 15,000 followers - a large number given their relatively recent creation date.



**dads doll** ❤️
@Evelynmuoki

We live ✨♨️

We love 💋❤️

We lie💔

DM strictly for business talk !!!!!!!
twin sister to @mdooolly

Born January 9, 2002 Joined March 2020

753 Following 34.7K Followers

**Kenya Finest** ❤️
@Queen_Maureen1

Proud Kenyan🇰🇪|●| LLB |●| Digital Marketer|●| #MUFC |●| DM for Anything, Business given Priority|●| Just for Fun✊😍

Nairobi, Kenya Joined April 2020

3,225 Following 35.6K Followers

**supu ya mutura**
@iamkuriah

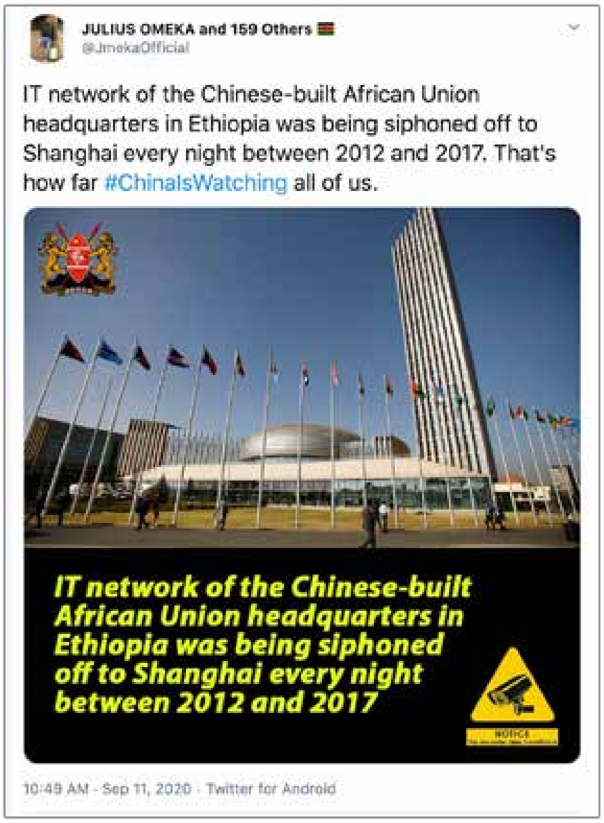
Your favorite Digital Marketer and Influencer. Dm for adverts, promos,business and trends.

kwa mathe Born October 30 Joined February 2020

3,412 Following 15.1K Followers

## China is Watching

The hashtag #ChinaIsWatching first appeared on Twitter in July 2012, in a sports-related tweet. Since then this hashtag has been used sporadically in different unrelated conversations by users across the world. A sudden spike in this hashtag was noted on 11 September 2020, led by a tweet by @JmekaOfficial, which claimed that the IT networks of the AU had been siphoned off to China between 2012 and 2017. This post was followed by an avalanche of posts with a similar narrative of China-led data harvesting.



JULIUS OMEKA and 159 Others 🇰🇪
@JmekaOfficial

IT network of the Chinese-built African Union headquarters in Ethiopia was being siphoned off to Shanghai every night between 2012 and 2017. That's how far #ChinaIsWatching all of us.

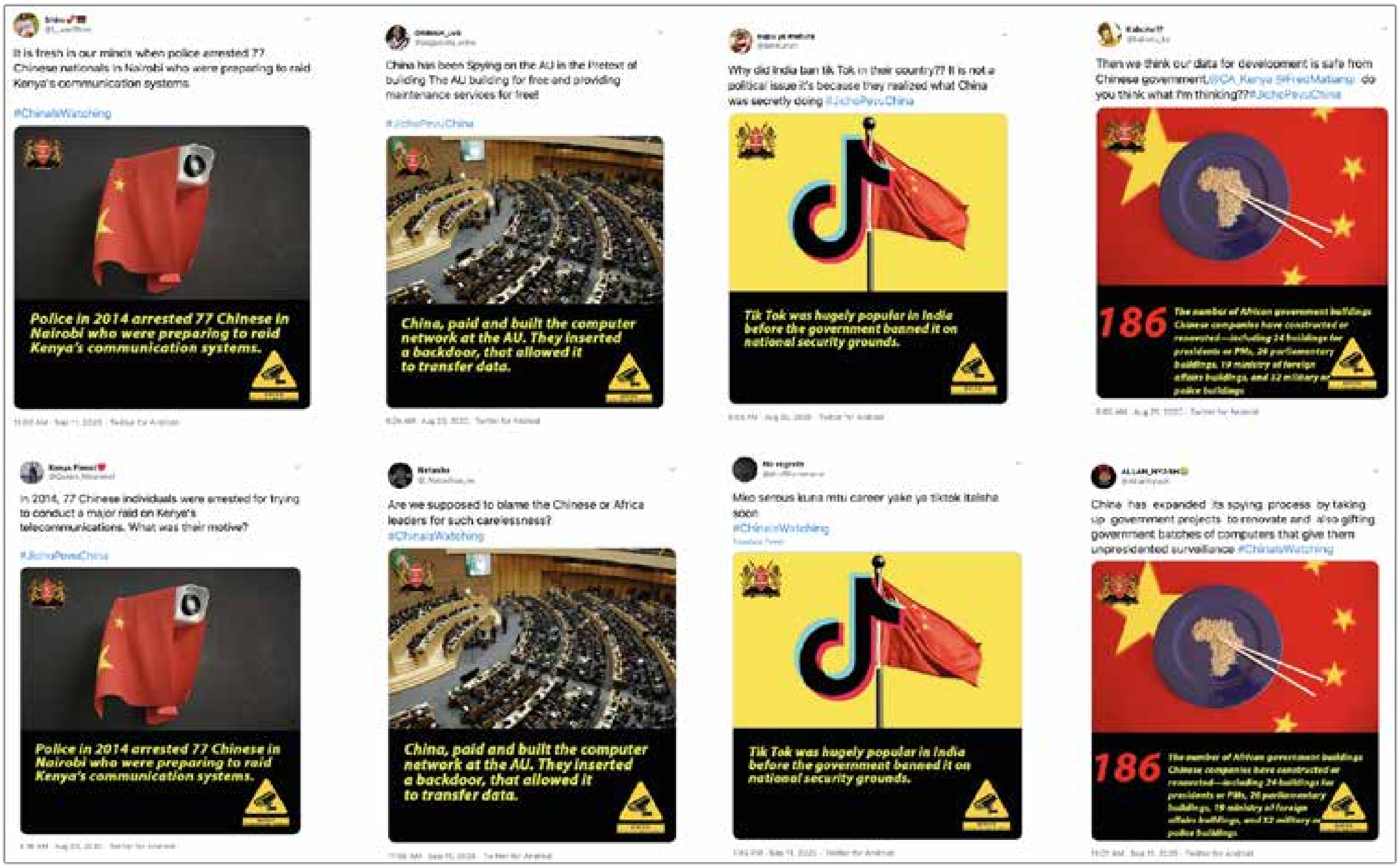
*IT network of the Chinese-built African Union headquarters in Ethiopia was being siphoned off to Shanghai every night between 2012 and 2017*

10:49 AM · Sep 11, 2020 · Twitter for Android

**Screengrab of the first tweet under #ChinaIsWatching's September 2020 spike (Source:Twitter/CfA)**

Similar to the previous campaign, a cluster of identical infographics were simultaneously uploaded. These infographics had a similar design to the earlier ones, with a number replicated from the previous campaign. The narratives replicated from #JichoPevuChina were:

- The 2014 arrest of 70 Chinese nationals in Nairobi over suspected cybercrime activity and the financial systems that could have been affected if this activity had not been discovered;
- The 2018 allegation of China spying on the AU through the IT network in the Chinese-built headquarters;
- India's TikTok ban;
- The 2020 Heritage Foundation report on China's alleged spying in Africa through the 186 government buildings and at least 14 sensitive intra-governmental telecommunication networks that it had constructed.



It is fresh in our minds when police arrested 77 Chinese nationals in Nairobi who were preparing to raid Kenya's communication systems

#ChinaIsWatching

Police in 2014 arrested 77 Chinese in Nairobi who were preparing to raid Kenya's communication systems.

China has been Spying on the AU in the Pretext of building The AU building for free and providing maintenance services for free!

#JichoPevuChina

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

Why did India ban tik Tok in their country?? It is not a political issue it's because they realized what China was secretly doing #JichoPevuChina

Tik Tok was hugely popular in India before the government banned it on national security grounds.

Then we think our data for development is safe from Chinese government, @CA_Kenya @FredMatiangi do you think what I'm thinking??#JichoPevuChina

186 The number of African government buildings Chinese companies have constructed or renovated—including 24 buildings for presidents or PMs, 26 parliamentary buildings, 19 ministry of foreign affairs buildings, and 32 military or police buildings

In 2014, 77 Chinese individuals were arrested for trying to conduct a major raid on Kenya's telecommunications. What was their motive?

#JichoPevuChina

Police in 2014 arrested 77 Chinese in Nairobi who were preparing to raid Kenya's communication systems.

Are we supposed to blame the Chinese or Africa leaders for such carelessness?
#ChinaIsWatching

China, paid and built the computer network at the AU. They inserted a backdoor, that allowed it to transfer data.

Mko serious kuna mtu career yake ya tiktok itaisha soon
#ChinaIsWatching

Tik Tok was hugely popular in India before the government banned it on national security grounds.

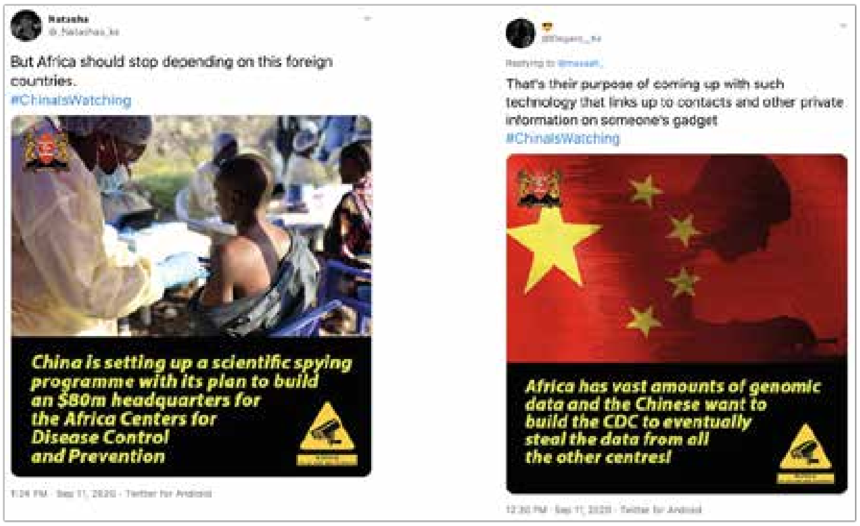
China has expanded its spying process by taking up government projects to renovate and also gifting government batches of computers that give them unpresidanted surveillance #ChinaIsWatching

186 The number of African government buildings Chinese companies have constructed or renovated—including 24 buildings for presidents or PMs, 26 parliamentary buildings, 19 ministry of foreign affairs buildings, and 32 military or police buildings

**Screengrab of the first tweet under #ChinaIsWatching's September 2020 spike (Source:Twitter/CfA)**

An analysis into the new narratives spread using the infographics led us to the following reports and incidents:

- **A 2020 US government allegation that China wants to steal African genomic data:** The US government alleges that China's involvement in the construction of the headquarters of the Africa Centres for Disease Control and Prevention (Africa CDC) is a front for a scientific spying program. This claim from the Trump administration, which has been dismissed by China, alleges that China is facilitating this construction so as to steal African genomic data. Two infographics were derived from this claim and were posted five times and retweeted 30 times.



Natasha
@_Natashas_ke

But Africa should stop depending on this foreign countries.
#ChinaIsWatching

China is setting up a scientific spying programme with its plan to build an $80m headquarters for the Africa Centers for Disease Control and Prevention

1:24 PM · Sep 11, 2020 · Twitter for Android

Replying to @masaai_

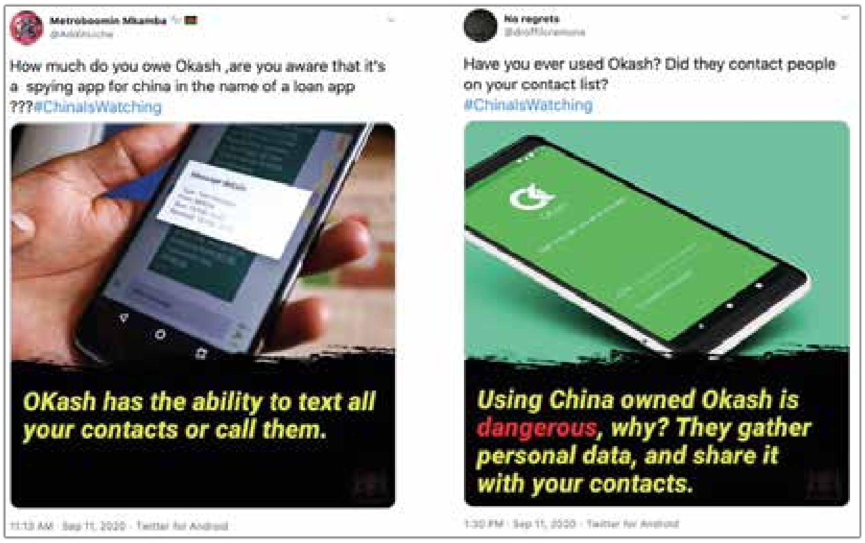
That's their purpose of coming up with such technology that links up to contacts and other private information on someone's gadget
#ChinaIsWatching

Africa has vast amounts of genomic data and the Chinese want to build the CDC to eventually steal the data from all the other centres!

12:30 PM · Sep 11, 2020 · Twitter for Android

- **Okash's debt recovery strategies:** Okash, a popular mobile loan app in Kenya, has faced public outcry, following revelations of its aggressive debt recovery strategies. Users of this platform have narrated how their phone contacts have been informed of their failure to repay their loans. Okash's app permissions and privacy policy allow for contact access, with the privacy policy highlighting that Okash "may also collect your email and phone-book contacts and information related to device activity such as call logs, SMS logs and GPS location information".

  Two infographics were derived from this: the first highlighted that Okash has the ability to message or call a user's contacts and was posted 18 times and retweeted 75 times. The second infographic highlighted that Okash shares personal data with a user's contacts. This was posted nine times and retweeted 52 times.



Metroboomin Mkamba

How much do you owe Okash ,are you aware that it's a spying app for china in the name of a loan app ???#ChinaIsWatching

OKash has the ability to text all your contacts or call them.

11:13 AM · Sep 11, 2020 · Twitter for Android

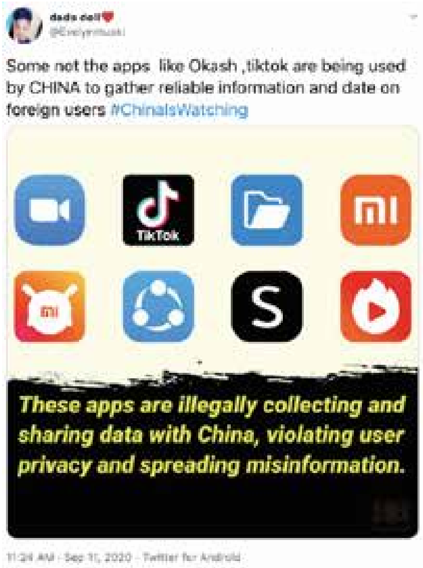
No regrets

Have you ever used Okash? Did they contact people on your contact list?
#ChinaIsWatching

Using China owned Okash is dangerous, why? They gather personal data, and share it with your contacts.

1:30 PM · Sep 11, 2020 · Twitter for Android

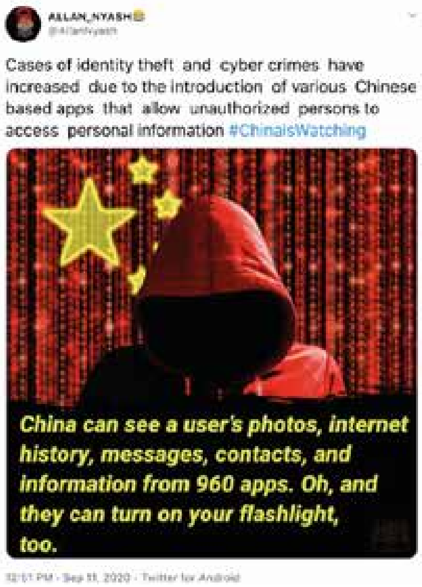
Apart from these incidents, we identified a narrative about apps allegedly sharing data with China. One of the infographics further alleged that China is capable of viewing a user's contacts, messages, photos and even operating the device's flashlight. Another infographic claimed that members of the China Communist Party (CCP) sit on TikTok's board. None of these allegations were backed by any evidence.


dada doll❤️
@Evelynmuoki

Some not the apps like Okash ,tiktok are being used by CHINA to gather reliable information and date on foreign users #ChinaIsWatching

*These apps are illegally collecting and sharing data with China, violating user privacy and spreading misinformation.*

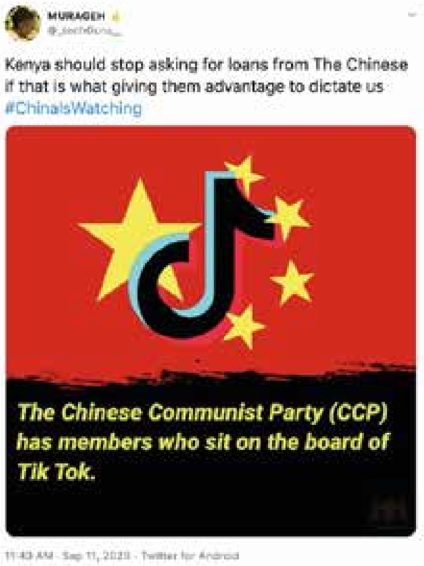
11:24 AM · Sep 11, 2020 · Twitter for Android


ALLAN_NYASH
@AllanNyash

Cases of identity theft and cyber crimes have increased due to the introduction of various Chinese based apps that allow unauthorized persons to access personal information #ChinaIsWatching

*China can see a user's photos, internet history, messages, contacts, and information from 960 apps. Oh, and they can turn on your flashlight, too.*

12:51 PM · Sep 11, 2020 · Twitter for Android

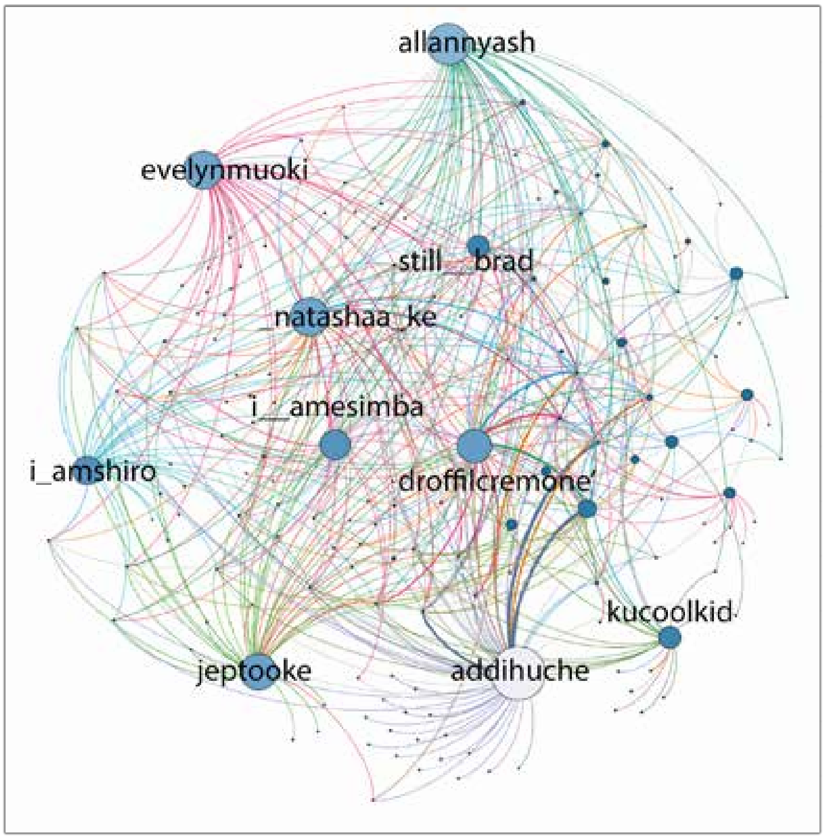

MURAGEH
@[illegible]

Kenya should stop asking for loans from The Chinese if that is what giving them advantage to dictate us #ChinaIsWatching

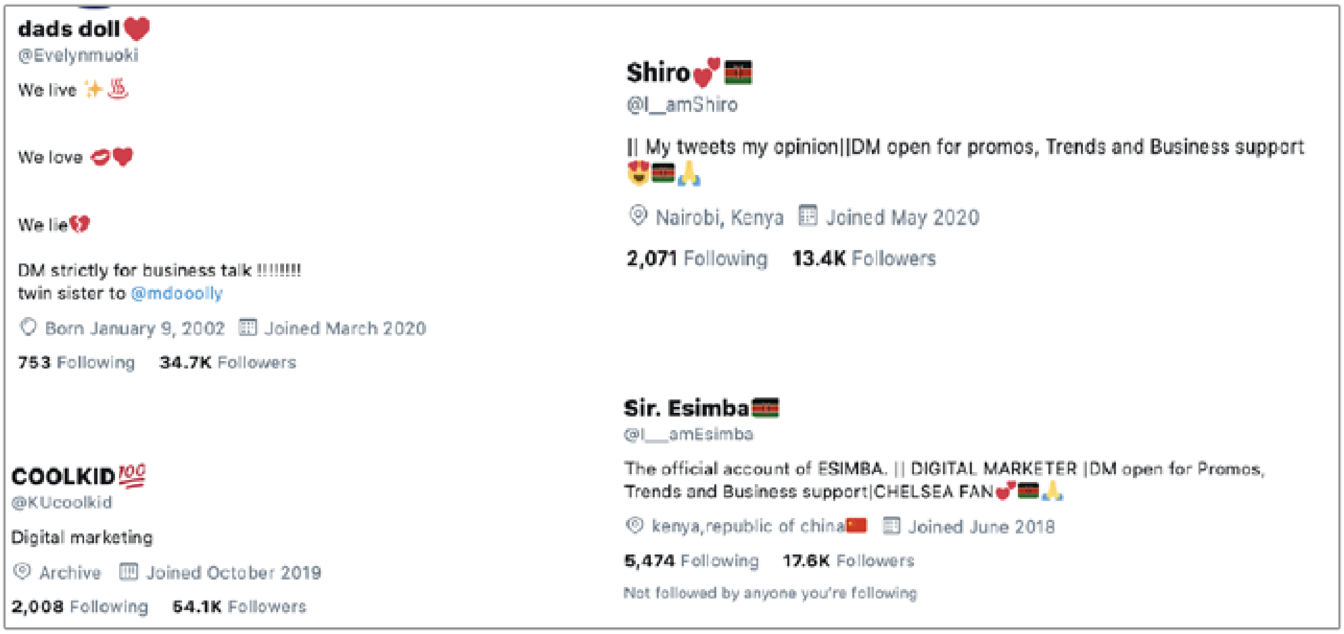
*The Chinese Communist Party (CCP) has members who sit on the board of Tik Tok.*

11:43 AM · Sep 11, 2020 · Twitter for Android

A network analysis of the accounts that posted and retweeted the infographics also shows a cluster of accounts acting as key amplifiers of these infographics. The highest number of posts came from @addihuche which posted 13 different images.



We observed that evelynmuoki and addihuche, key drivers of this narrative, had also participated in #JichoPevuChina. Similar to the previous trend, an analysis of the profiles of the key accounts revealed that the drivers of these narratives are online marketers, simply pushing a trend.



**dads doll❤️**
@Evelynmuoki
We live ✨♨️

We love 💋❤️

We lie💔

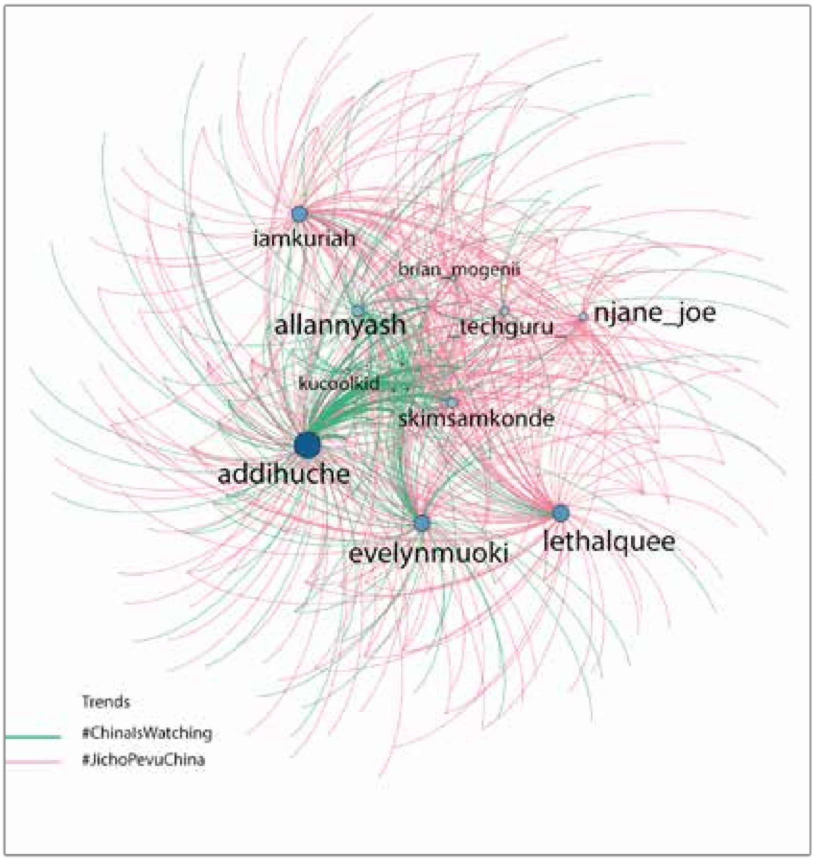
DM strictly for business talk !!!!!!!
twin sister to @mdooolly
Born January 9, 2002 Joined March 2020
753 Following 34.7K Followers

**Shiro💕🇰🇪**
@I_amShiro
|| My tweets my opinion||DM open for promos, Trends and Business support 😍🇰🇪🙏
Nairobi, Kenya Joined May 2020
2,071 Following 13.4K Followers

**Sir. Esimba🇰🇪**
@I__amEsimba
The official account of ESIMBA. || DIGITAL MARKETER |DM open for Promos, Trends and Business support|CHELSEA FAN💕🇰🇪🙏
kenya,republic of china🇨🇳 Joined June 2018
5,474 Following 17.6K Followers
Not followed by anyone you're following

**COOLKID💯**
@KUcoolkid
Digital marketing
Archive Joined October 2019
2,008 Following 54.1K Followers

A combined analysis of the two trends revealed a cluster of 249 accounts that participated in the coordinated image sharing in both hashtags. Given the identical narratives, actors and profiles observed in the two trends, our analysis leads us to conclude that this was a coordinated attack on China's activities in Kenya and Africa as a whole.



# Conclusion

This investigation has revealed a coordinated Twitter attack against China's investments and activities in Africa. The perpetrators of this false narrative leveraged on past incidences, unbacked claims and controversies surrounding China's involvement in Africa, to spread a tale of a continent under unwanted, unwarranted surveillance. It is unclear as to who is the exact instigator of this campaign; but the timing and behaviour of the campaign's participants strongly point to a larger ulterior motive.

# Recommendations

## Newsrooms should consider the following:

1. Setting up investigative desks with dedicated teams;
2. Upscaling the investigative skills of the internal teams to conduct investigations into co-ordinated inauthentic behaviour;
3. Monitoring of social media platforms to identify trends that have indicators of manipulation;
4. Conducting follow-up and additional investigation to identify key puppet masters, given that the behaviour observed in this investigation is ongoing;
5. Adopting the factual findings reporting structure for published articles to ensure supporting evidence is available for investigative reports.

## Published by

Code for Africa is the continent's largest federation of civic technology and data journalism labs with teams in: Burundi, Ethiopia, Ghana, Kenya, Morocco, Mali, Nigeer, Nigeria, Senegal, Sierra Leone, South Africa, Tanzania, Tunisia & Uganda

CfA Secretariat: 112 Loop Street, Cape Town, Western Cape, 8000, South Africa.
South Africa NPO Number 168-092 | Kenya NPO Number CPR/2016/220101 | Nigeria NPO Number: RC-1503312
Kenya Lab: Nairobi Garage, 8th Floor, Pinetree Plaza, Kaburu Drive, Nairobi, Kenya.
Nigeria (Abuja) Lab: Ventures Park, 29,Mambilla Street, Aso Drive, Abuja, Nigeria.
Nigeria(Lagos) Lab: Workstation, No 7, Ibiyinka Olorunbe street, off Saka Tinibu, Victoria Island, Lagos, Nigeria
Tanzania Lab: 7th Floor, 38 Tanzanite, Park, New Bagamoyo Road, Dar es Salaam, Tanzania.
Uganda Lab Pollicy, Plot 7 Kulubya Road, Bugolobi, Kampala, Uganda.

CODE for AFRICA academy AFRICA DW Akademie