



# Graphika

## Fake Cluster Boosts Huawei

Accounts with GAN Faces Attack Belgium  
Over 5G Restrictions

Graphika Team

**01.2021**

**Information Operations**

# Fake Cluster Boosts Huawei

Accounts with GAN Faces Attack Belgium over 5G Restrictions

## Executive Summary

- A cluster of inauthentic accounts on Twitter amplified, and sometimes created, articles that attacked the Belgian government's recent [plans](#) to limit the access of "high-risk" suppliers to its 5G network. The plans are [reportedly designed](#) to limit the influence of Chinese firms, notably Huawei and ZTE.
- The operation appears to have been limited to Twitter, and it did not gain substantial traction: other than a systematic amplification by the real accounts of Huawei executives in Western Europe, its main amplification came from bots with zero followers.
- As so often in recent influence operations, the accounts used profile pictures created by artificial intelligence.
- There is insufficient forensic evidence to prove conclusively who was running the fake accounts, or who sponsored the operation.

## Fakes with GAN faces

Graphika first came across this network in early December in the course of the continuing investigation of the [Spamouflage](#) network. (Independently, Belgian researchers [@bickylover](#) and [Michiel van Hulten](#) came across the same network when its promoted tweets appeared in their feeds.)<sup>1</sup> A handful of Spamouflage accounts retweeted an account called @alexandre\_phd, with a stated location in Brussels and posting in English about the Belgian 5G decision and its many negative consequences.

---

<sup>1</sup> While this report was being drafted, we were made aware of an article on Belgian Dutch-language [website knack.be](#) that reported on the same cluster and made many of the same findings, including the presence of fake accounts, articles attributed to those fake accounts, and amplification by Huawei executives.



Tweets by @alexandre\_phd, December 16-18, 2020.

By examining this account and the articles it shared, Graphika found 13 more accounts that had an identical behavior pattern. All posted the same handful of articles with different comments on the Belgian 5G decision, interspersed with retweets on a range of tech-related subjects.



*Profiles of the 14 accounts in the Twitter cluster. The top left account used for its banner a photo of two children; we have obscured their faces to protect their privacy.*

All 14 had profile pictures that appear to have been created using the form of artificial intelligence known as Generative Adversarial Networks (GAN), a technique that has become endemic among influence operations in the past year and a half. To date and despite the rapid developments of GANs, most of these images can still be identified by a range of features, notably asymmetries on both sides of the faces and a lack of detail in the background. In the case of images produced by the same software, one can also lower the opacity of each image and superimpose them on each other: in this case, the eyeballs of all 14 profile pictures used by the inauthentic accounts aligned perfectly.



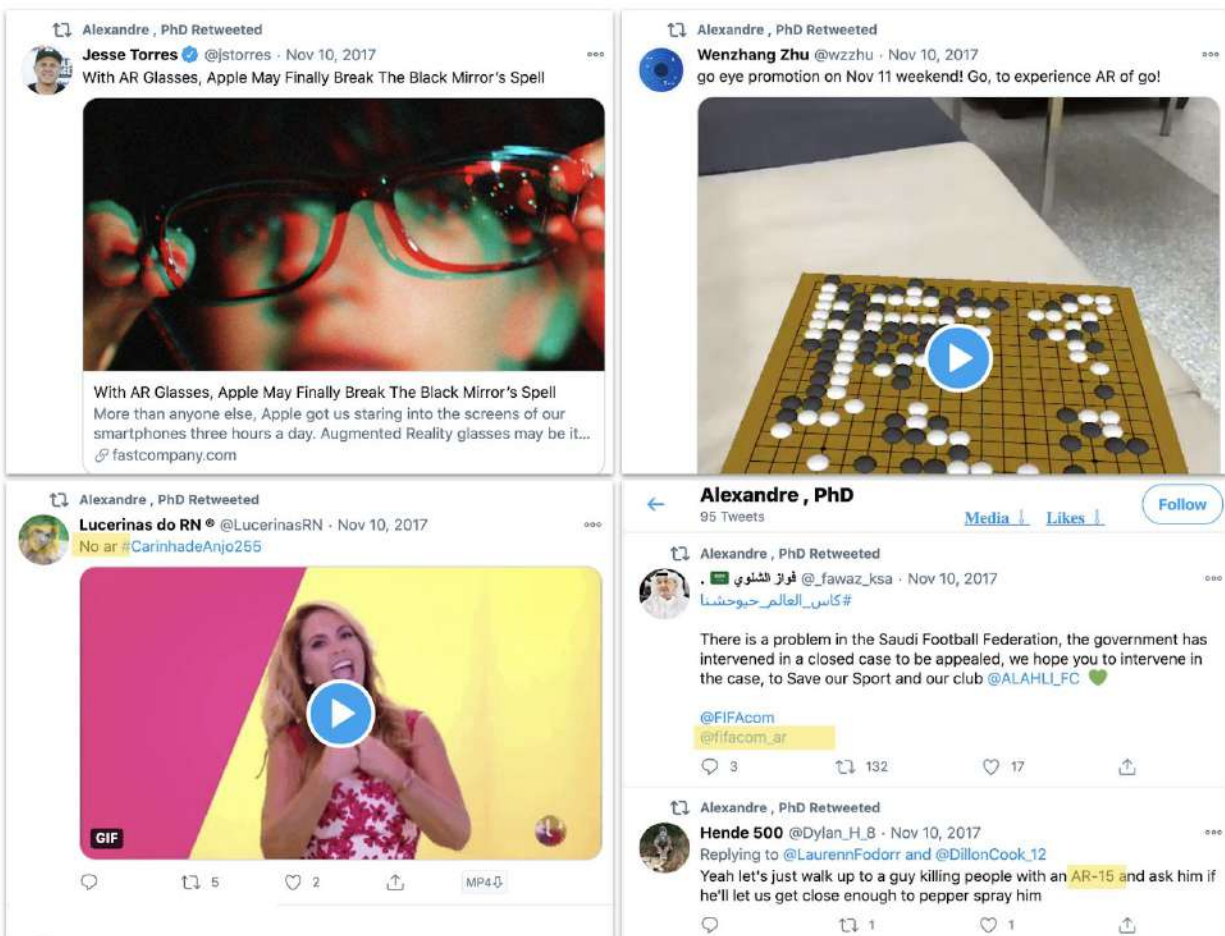
*The profile pictures of the 14 pro-Huawei accounts, made opaque and superimposed.*

Each of these fake accounts had very similar behavior. They were created in the second half of 2017, but only started tweeting in late 2020. Despite the late date at which they started tweeting, their first posts were all retweets of tech-related content that originated on November 10, 2017 or November 10, 2018. This is likely to have been an attempt to make them look as if they had been in use for a long time, and to give them the appearance of tech-focused accounts. On each account, most of the retweeted posts used the same keyword or hashtag, such as "VR" (virtual reality), "AR" (augmented reality) or "5G". The tweets were not always relevant to the tech world, suggesting that they may have been automated and not manually checked - for example when

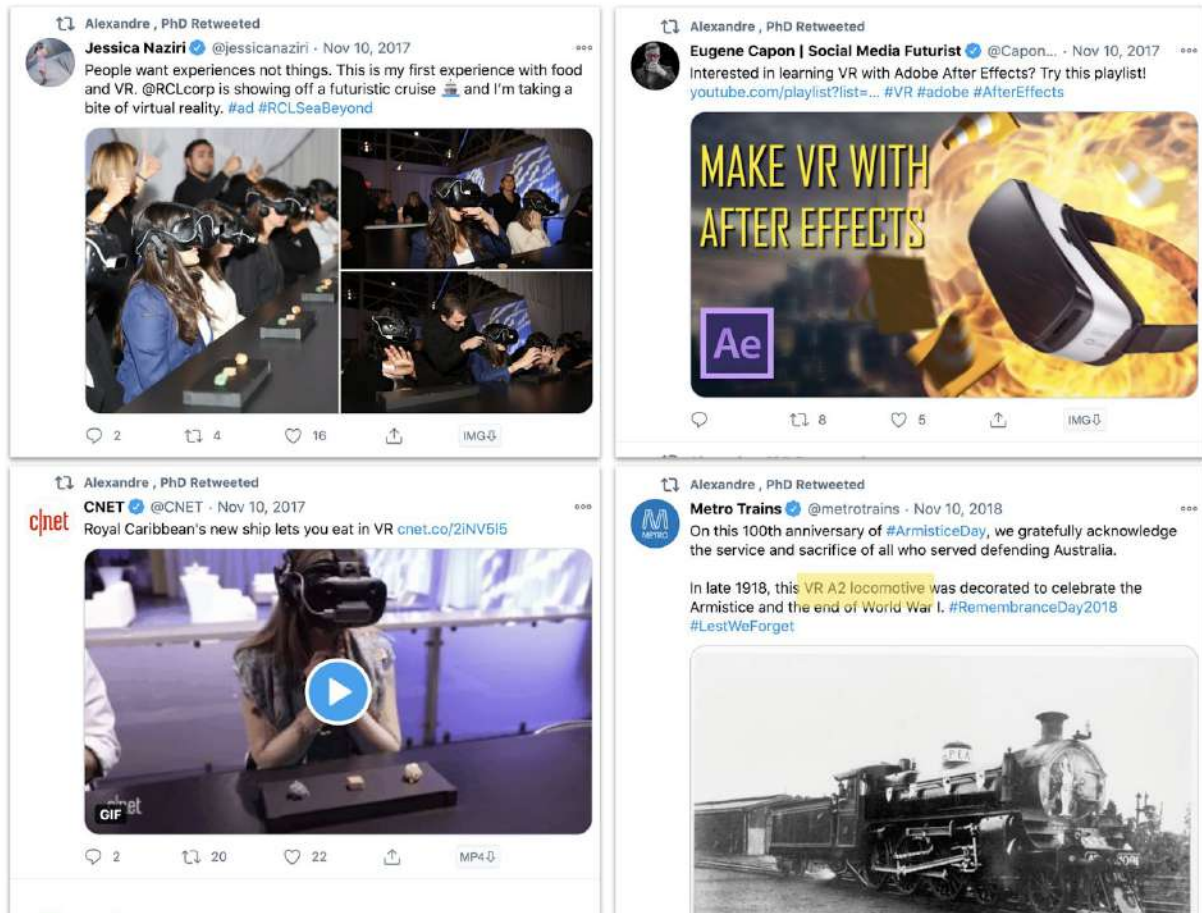
@alexandre\_phd retweeted a post about VR that actually concerned Australia's [Victorian Railways](#).



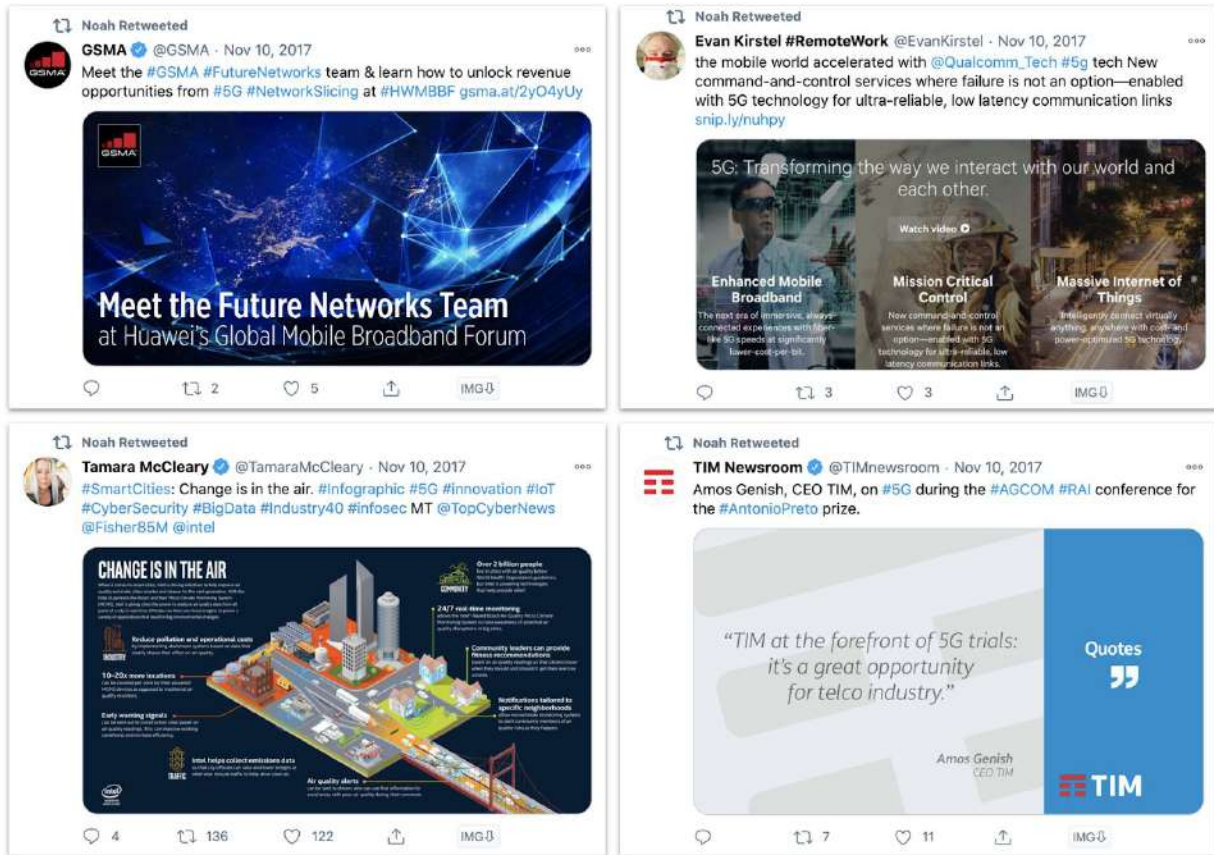
Profiles of @alexandre\_phd and @lanNoah11; note the creation dates. @lanNoah11 is an oddity as a "bestselling author, editor, journalist" whose timeline made no mention of any of his apparently bestselling books.



The first retweets by @alexandre\_phd. The theme of these retweets appears to have been AR, but the tweets chosen included mentions of FIFA's Arabic account and the AR-15 assault weapon.

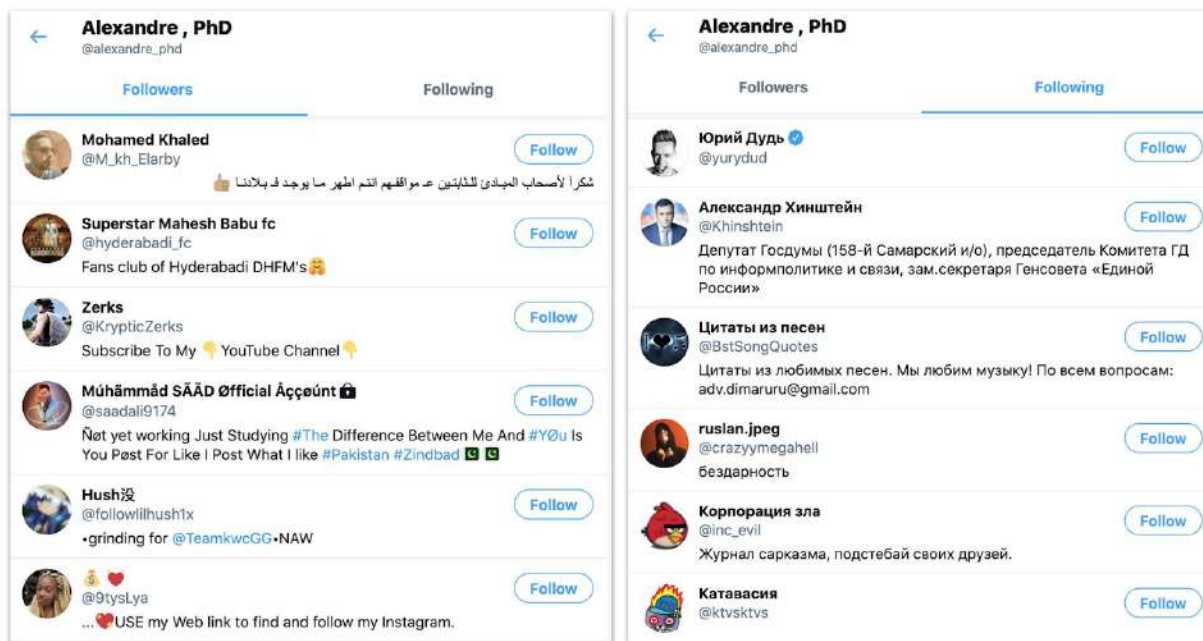


Early retweets by @alexandre\_phd that contain the term "VR," including one anomalous tweet about Victorian Railways.



Early retweets by @lanNoah11, on 5G.

Each of these fake accounts had at least 1,800 followers, but the vast majority came from countries and language groups that were incongruous for users who were ostensibly based in Belgium. They each followed at least 40 other accounts, but these also showed a language bias away from French or Dutch, and towards languages that included Russian and Arabic. This suggests that the fake accounts were equipped with fake followings, purchased online from international suppliers without too much thought given to verisimilitude.



Left, followers of @alexandre\_phd. Right, the first accounts followed by this account.

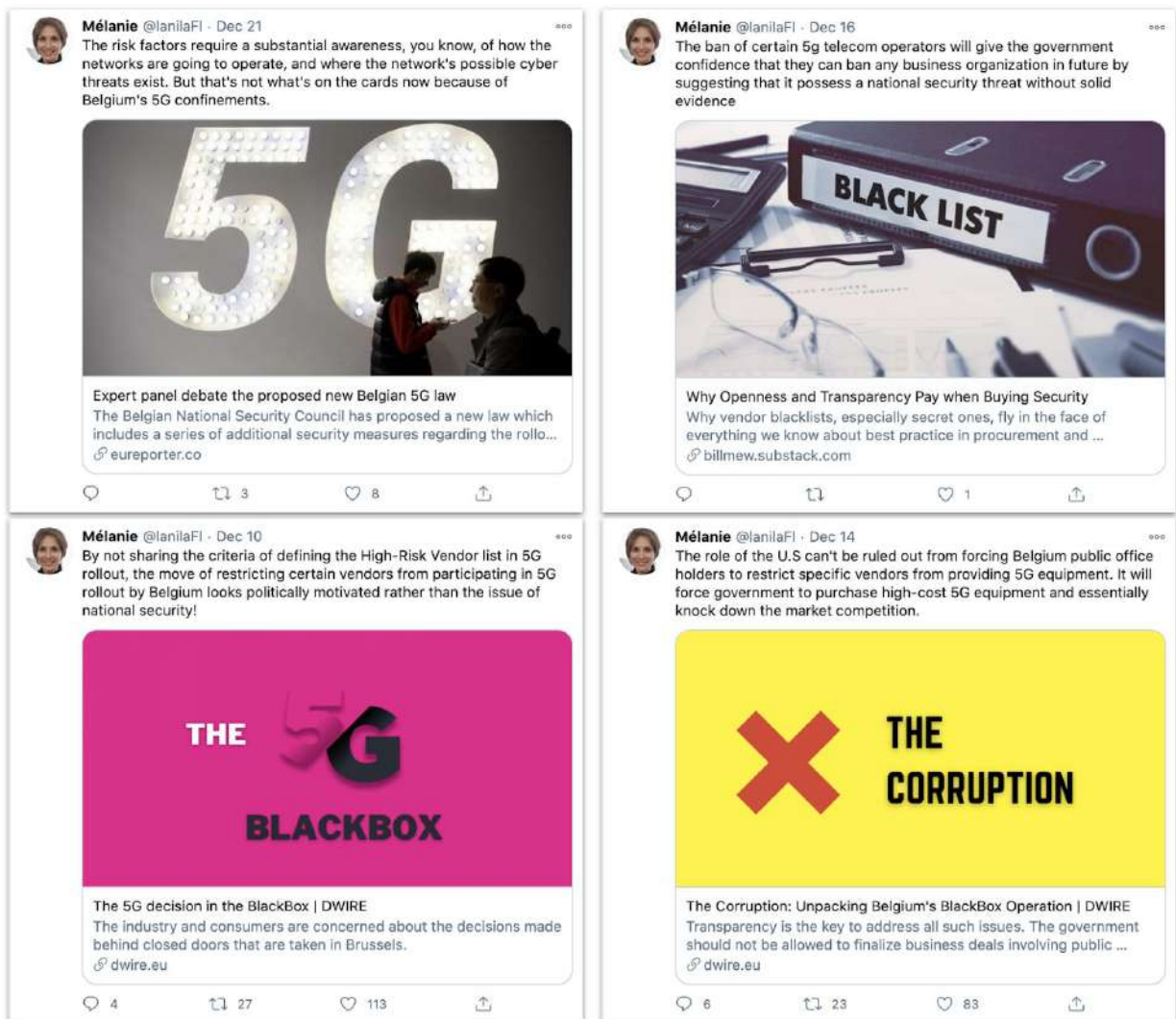
## Anti-Belgium, Pro-5G, Pro-Huawei

In between the retweets, each of the 14 accounts in this set tweeted links to articles about Belgium's 5G decision and why it was a bad idea, or articles about Huawei and why it was a reliable investor and partner. The articles came from a range of sources, including Politico, German business paper Handelsblatt, and the websites eureporter.co and dwire.eu. Each account tweeted the same articles, with different comments to accompany them. This tweeting appears to have been manual rather than automated, and the text of the tweet was different in each case.

By December 23, each of the accounts had posted 8-10 authored tweets in between several dozen retweets of tech-related content.



Authored tweets by @NoriceMaslen, praising Huawei (top and bottom right) and calling the Belgian government corrupt (bottom left). The bottom right post was a [sponsored article](#) by Sophie Batas, the director for cybersecurity at Huawei EU, on Politico.



*Authored tweets by @lanilaFL (screen name Melanie) accusing Belgium of corruption and politically motivated decisions "rather than the issue of national security!"*

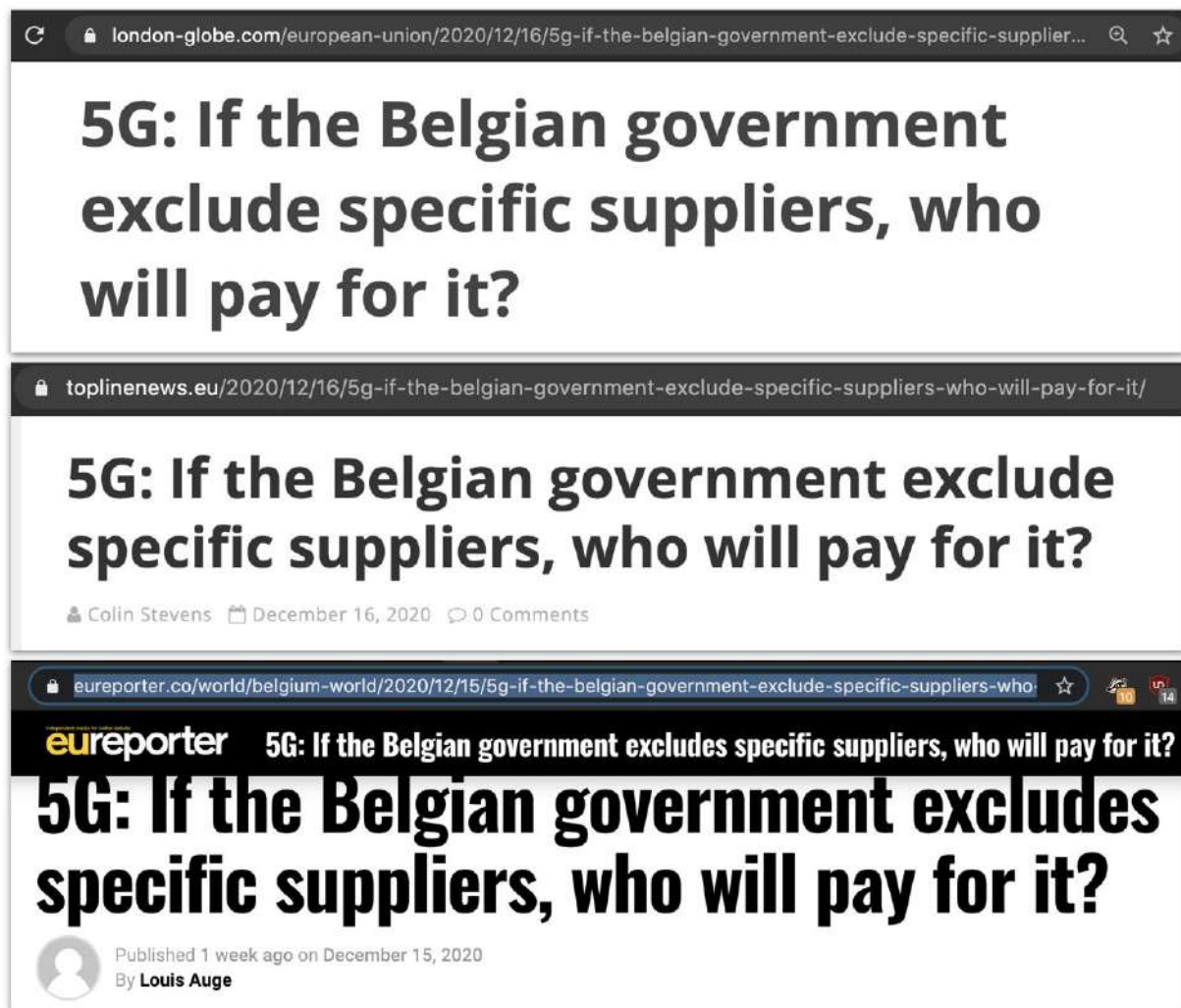
## Same Script, Different Domains

Among the articles that the fake accounts promoted were a few cases in which the same article appeared on multiple, apparently connected, websites at the same time. On these occasions, the fake accounts in the network took advantage of this fact to tweet the same headline from different sites, thus making it less likely that a URL-based search would be able to identify them all as a network. (The websites in question long pre-dated this operation; there is no forensic evidence to suggest that they were knowingly involved in the operation.)

For example, all the accounts shared an article headlined, "5G: If the Belgian government exclude specific suppliers, who will pay for it?"

"Compared with other EU countries with sufficient competition, such as Germany, the Netherlands, Spain, etc., Belgian consumers will pay higher fees for this. In the post-epidemic era, this will put tremendous pressure on Belgium's economic recovery," argued the article, which also quoted an unnamed "mobile network CEO" as saying the Belgian move was aimed at Huawei and ZTE.

This article appeared on four different websites: [london-globe.com](http://london-globe.com) and [newyorkglobe.co](http://newyorkglobe.co), where it was not bylined; [toplinenews.eu](http://toplinenews.eu), where it was bylined Colin Stevens; and [eureporter.co](http://eureporter.co), where it was bylined Louis Auge. These two names are [both listed](#) as regular contributors at eureporter.co. According to a [report](#) in the Sunday Times, london-globe.com, eureporter.co and newyorkglobe.co are "all small news websites privately owned by a small British company which is owned by a former TV journalist."



*The same headline on three different websites, with two different authors named.*

Many of the accounts in the network tweeted at least one version of this article, but not from the same source: most used the [toplinenews.eu](https://toplinenews.eu) version, but some tweeted the [eureporter.co](https://eureporter.co) one, and some shared the version at [london-globe.com](https://london-globe.com).

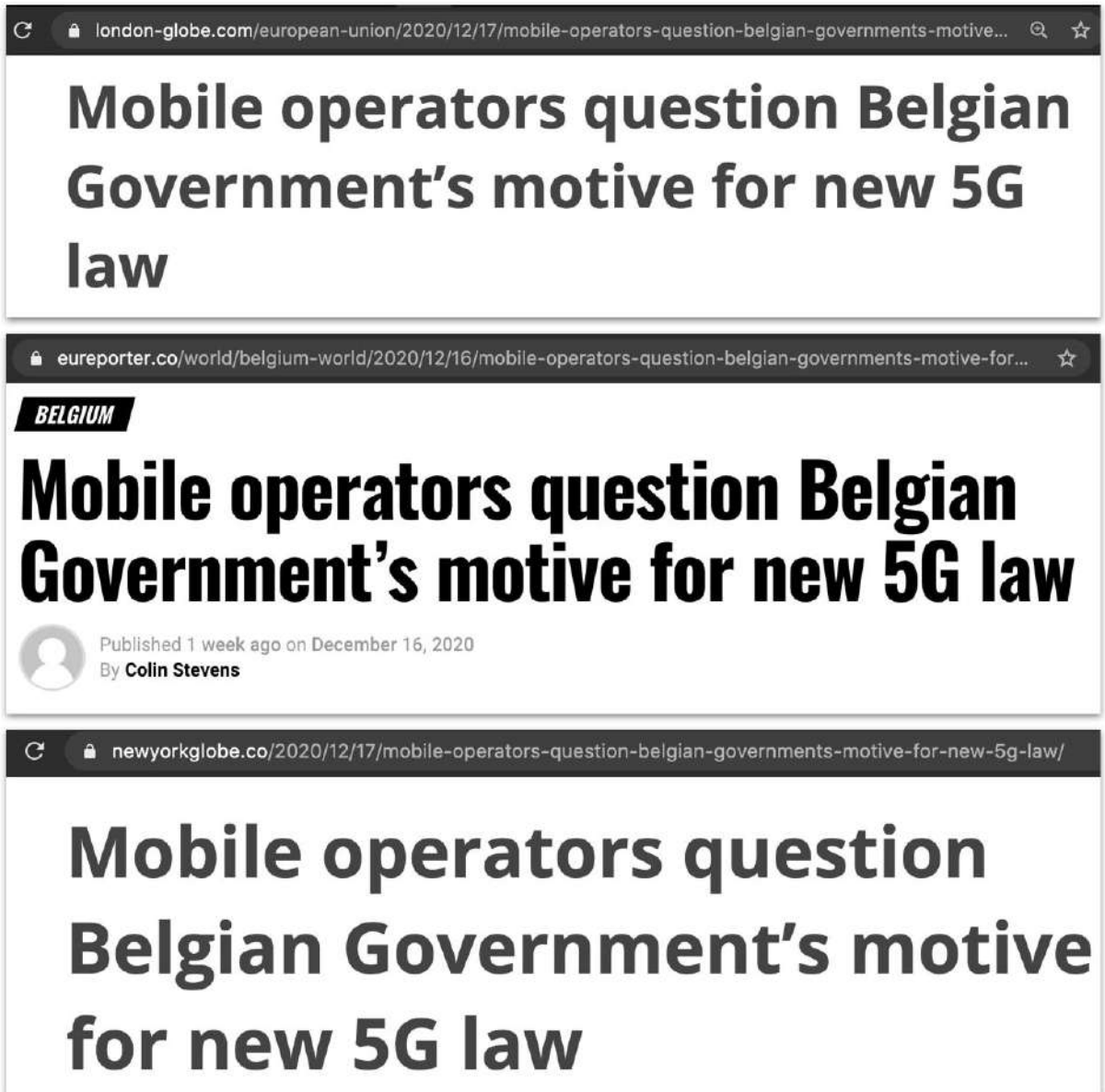


*Tweets of the same article from different sources, posted by different members of the network.*

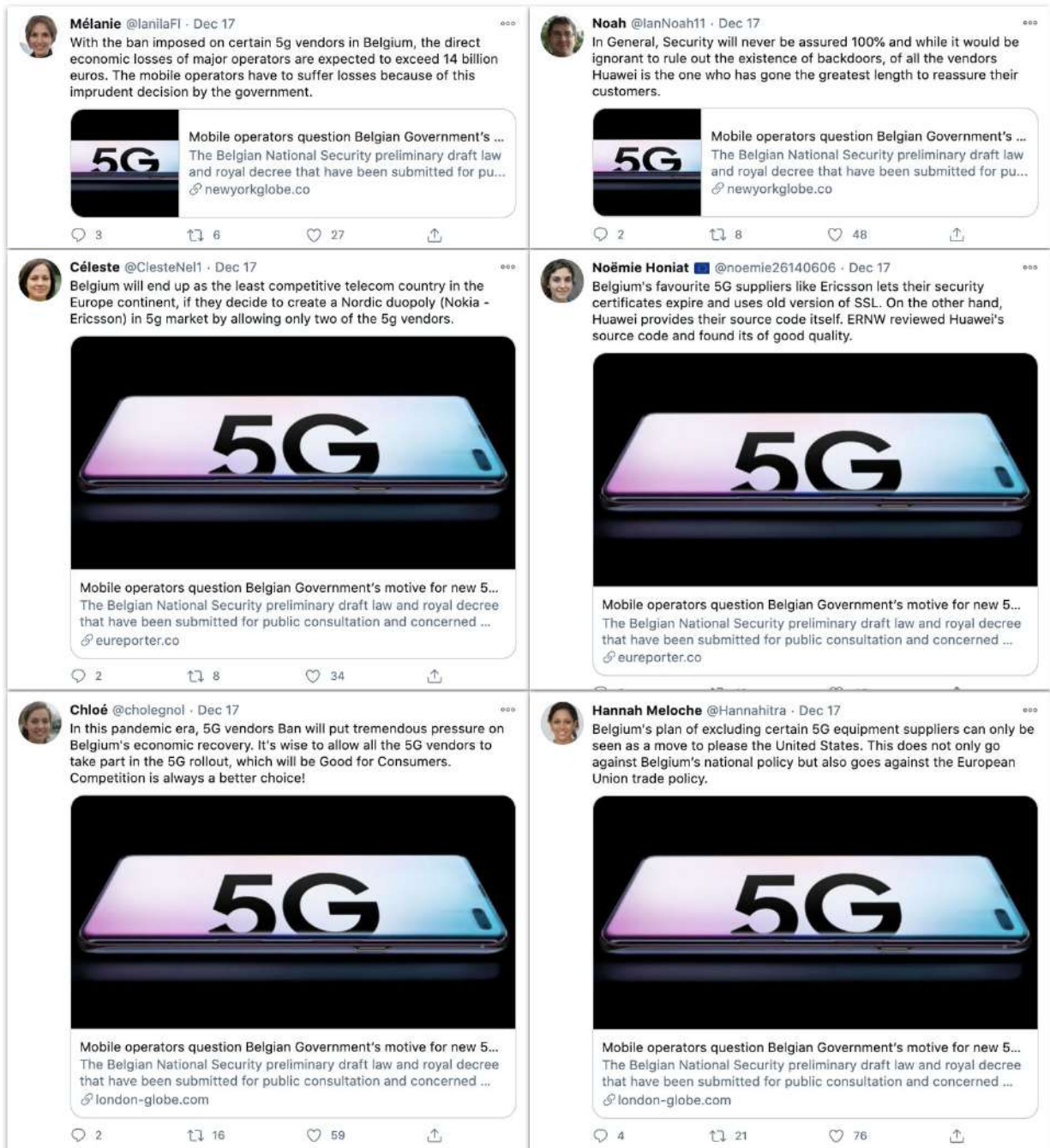
Another article was headlined, "Mobile operators question Belgian Government's motive for new 5G law." It was published on [london-globe.com](https://london-globe.com) without a byline, [eureporter.co](https://eureporter.co) under the byline of Colin Stevens, and [newyorkglobe.co](https://newyorkglobe.co) without a byline.

The Belgian proposal "is believed to be a cynical media manipulation tactic" which "could result in gravely impacting the swiftness of 5G rollout and the cost of 5G equipment could go remarkably high. Who is going to suffer from this situation the most? Of course, the consumer," the article

wrote. Again, it quoted two unnamed mobile-phone network CEOs, and argued that “of all the vendors Huawei is the one who has gone the greatest length to reassure their customers.”



*The same headline on three different websites.*



Different assets in the operation sharing the versions from (top to bottom) newyorkglobe.co, eureporter.co and london-globe.com.

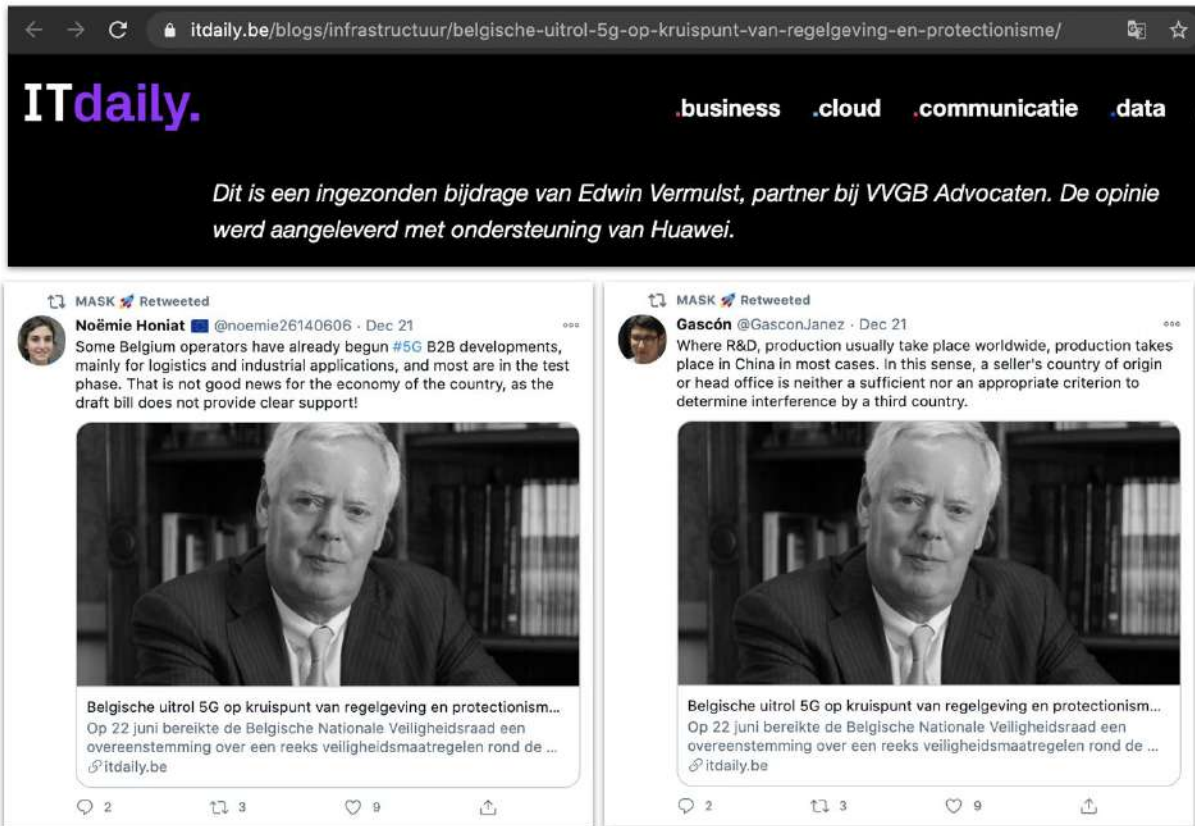
## Sponsored Content

On two occasions, the fake accounts shared articles that had been sponsored by Huawei. On December 28, many of them tweeted a link to an [article](#) on Politico that was headlined, “Huawei and European industry: natural partners.” The post was sponsored by Huawei and written by its EU Director for Cybersecurity, Sophie Batas.



*Operation accounts @lanilaFL and @IdaArlise tweeting a link to the sponsored post on Politico, together with the headline and (inset) the sponsorship notice.*

A week earlier, the operation’s accounts shared a link to a Dutch-language article whose headline translated as, “Belgium’s rollout of 5G at the crossroads of regulation and protectionism.” This was a [guest contribution](#) on one Belgian tech-focused website, called itdaily.be. A disclaimer at the end confirmed that it, too, was sponsored by Huawei.



Top, the disclaimer at the end of the article on itdaily.be, showing the Huawei support ("med ondersteuning van Huawei"). Bottom, two of the operation accounts that tweeted it.

## Written by Fakes

In two other cases, the operation's Twitter accounts amplified articles that were likely crafted by the operation itself. Both of these were posted on the blogging site dwire.eu. This [website](#) gives its street address as 84 Crescent de l'Europe 3, 1000 Brussels, but no such address seems to exist, according to a review of Google maps and a Brussels street atlas.

# Contact Information

84 Crescent de l'Europe 3, 1000  
Brussels, Belgium

✉ [contact@dwire.eu](mailto:contact@dwire.eu)



84, Crescent de l'Europe 3, Bruxel



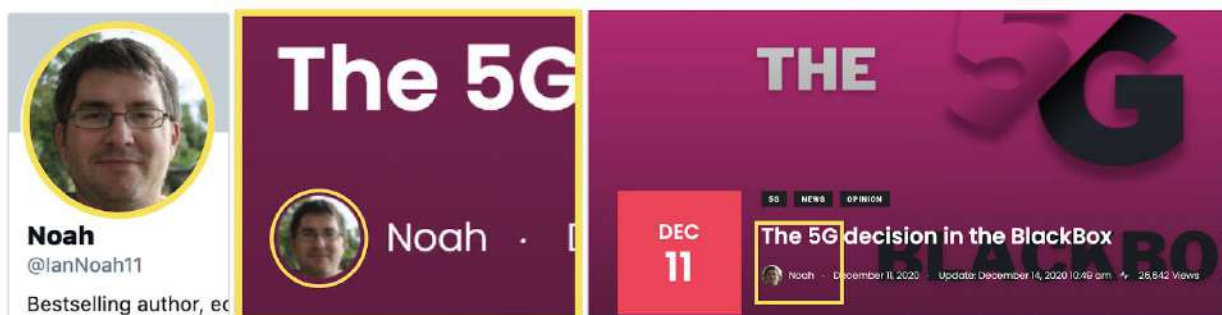
[Add a missing place to Google Maps.](#)

*Top, the address from the dwire.eu website's [Contact Information](#) section. Bottom, Google maps result of searching for the address, showing it as a missing place.*

The [first](#) of the two articles, published on December 11, called Belgium's 5G decision a "blackbox operation," and argued that the security procedure to define "high-risk vendors" should be thrown open to the public.

"The industry and consumers are concerned about the decisions made behind closed doors that are taken in Brussels. There is only one way to address the issues of national security concerns, make the whole process of defining the high-risk vendor list open to the public for debate. It is high time the national governments realize that transparency is the key to move forward in the right direction as nothing good comes out of closed doors decisions. People have a right to know what their governments are planning and doing with the future of their country. One of my friend [sic] said: 'No one in Belgium would like Blackbox operation'. **It seems that Brussels is being pressurized by a foreign entity to block certain 5G suppliers,**" it wrote (emphasis in the original).

The article was bylined “Noah,” and featured the same GAN-generated profile picture as that of the Twitter account @IanNoah11. This suggests that the article was most likely created by the operation itself, using one of the inauthentic personas profile pictures that it had generated.



Left to right, @IanNoah11 on Twitter, detail of the byline on dwire.eu, and the full headline.

Three days later, another [article](#) took the argument a step further by accusing Belgium of corruption. The headline ran, “The Corruption: Unpacking Belgium’s BlackBox Operation.” The article argued that “A recent example of such a deal is the plan to exclude some 5G equipment suppliers. This exclusion is based on a High-Risk Vendor list, that is being prepared by the Intelligence agencies of Belgium and was kept as a secret. This whole process is acknowledged as a Blackbox Operation by the Belgian government because of political pressure by the US. As the US incapable [sic] of providing advanced 5G equipment at a low cost so they want to kill the market competition.” It cited the “Noah” article as its source.

This article was attributed to “Melanie,” whose screen name and GAN profile picture matched operation asset @lanilaFL. Again, this suggests that the operation most likely created this article using another of its fake personas.



Left to right, @lanilaFL, detail of the “Melanie” byline, and the full headline.

These two articles show the operation not just amplifying politically angled content, but creating and planting that content online. It is noteworthy that neither @lanilaFL nor @IanNoah11 mentioned their claimed authorship when they tweeted the articles (unusual for accounts that both claimed to be authors): they simply added pointed comments about Belgium and the United States.



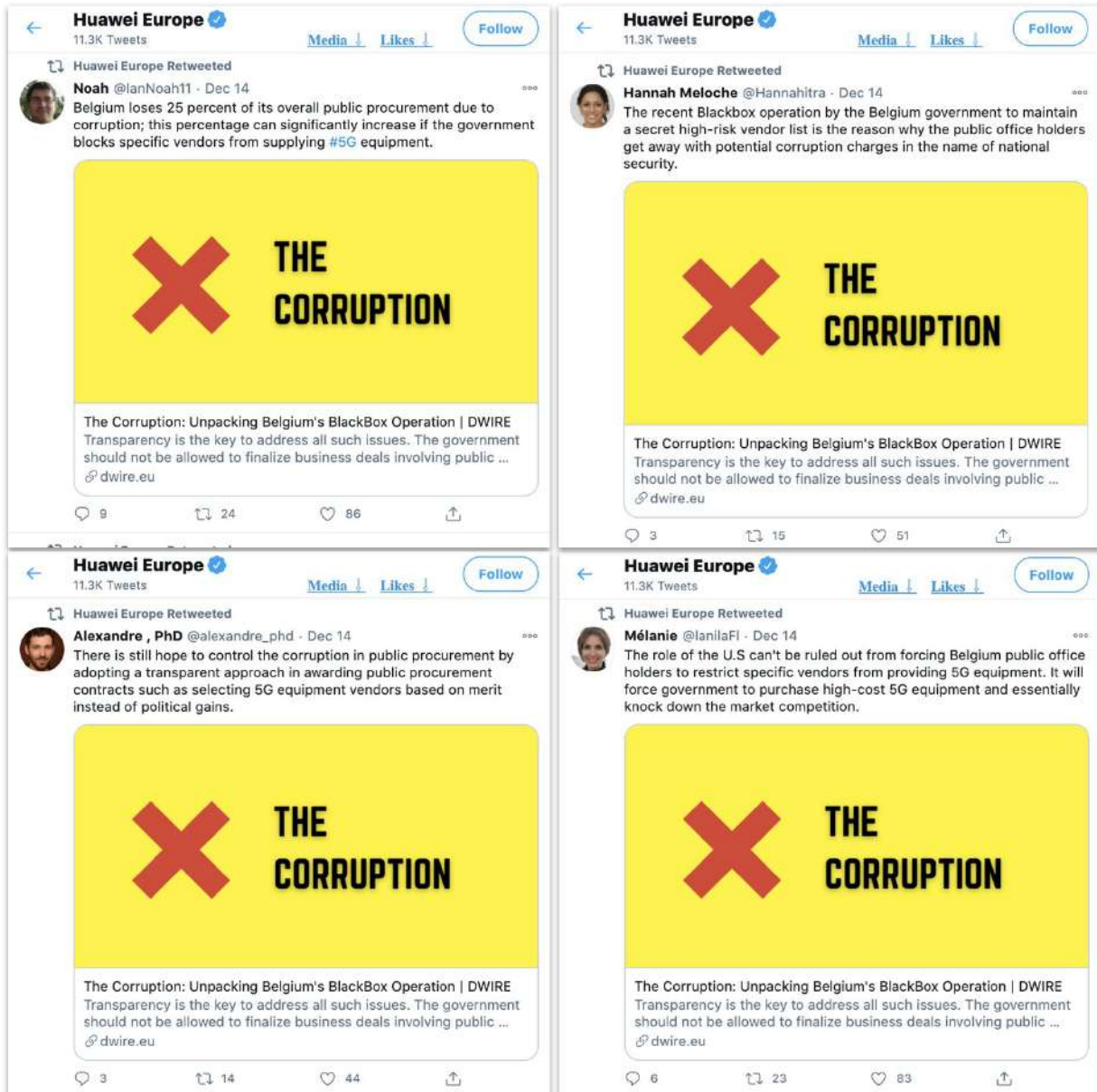
*Tweets by @lanilaFI and @lanNoah11 boosting the articles in their names; note how neither claims the authorship on Twitter.*

## Huawei Boosts Back

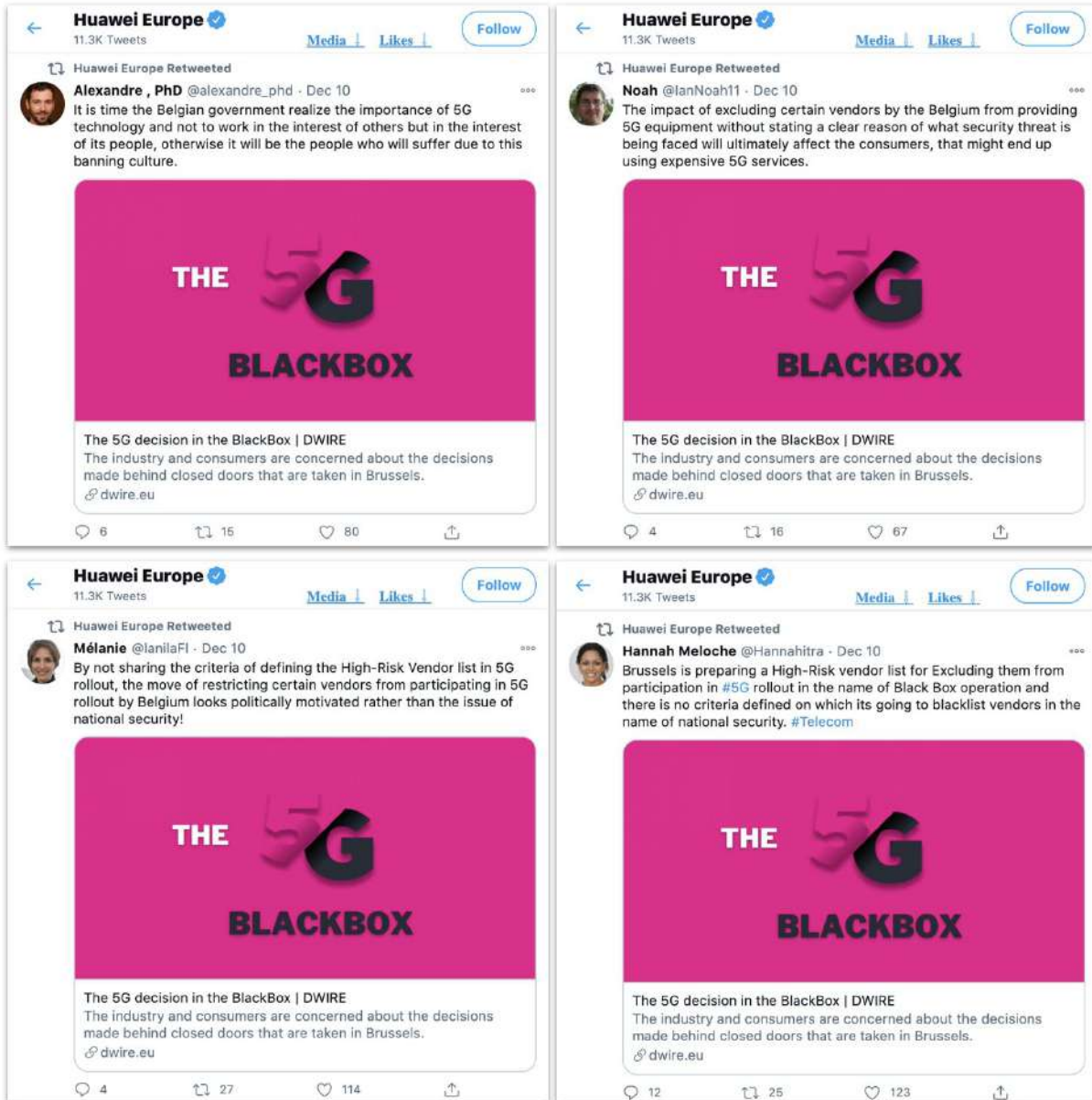
The above activity all stemmed from a small cluster of fake accounts whose origin could not be definitively identified at this stage. Their messaging was clearly anti-Belgium's 5G policies and, to a lesser extent, pro-Huawei, and they used a mixture of authentic news reporting, content paid for by Huawei, and articles they created themselves to make their points. This is not sufficient to suggest that Huawei itself or its personnel either conducted the operation or sponsored it in any way.

However, it is clear that these fake accounts' most important amplification came from Twitter accounts that belong to senior Huawei executives in Western Europe, including three accounts that are verified.

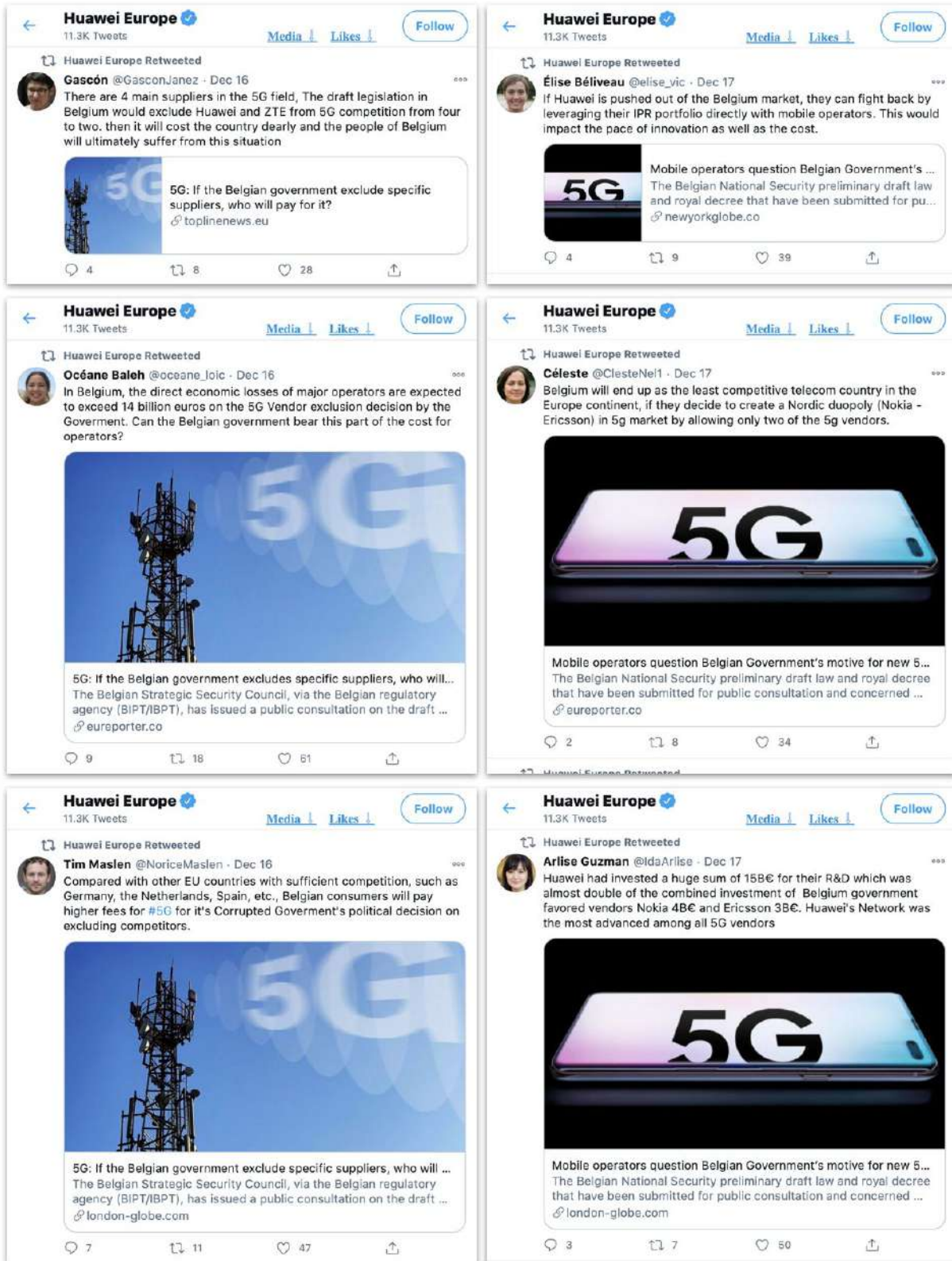
One of these was the corporate Twitter account of Huawei Europe itself. Rather than sharing each article once, the Huawei account retweeted multiple shares of the same article from multiple members of the network, including both of the articles that were planted by the inauthentic personas discussed above. In cases where the operation's fake accounts tweeted the same article from three different domains, the Huawei Europe account retweeted all three variants.



The verified account for Huawei Europe sharing four tweets of the same "Belgian corruption" article from different assets in the operation.

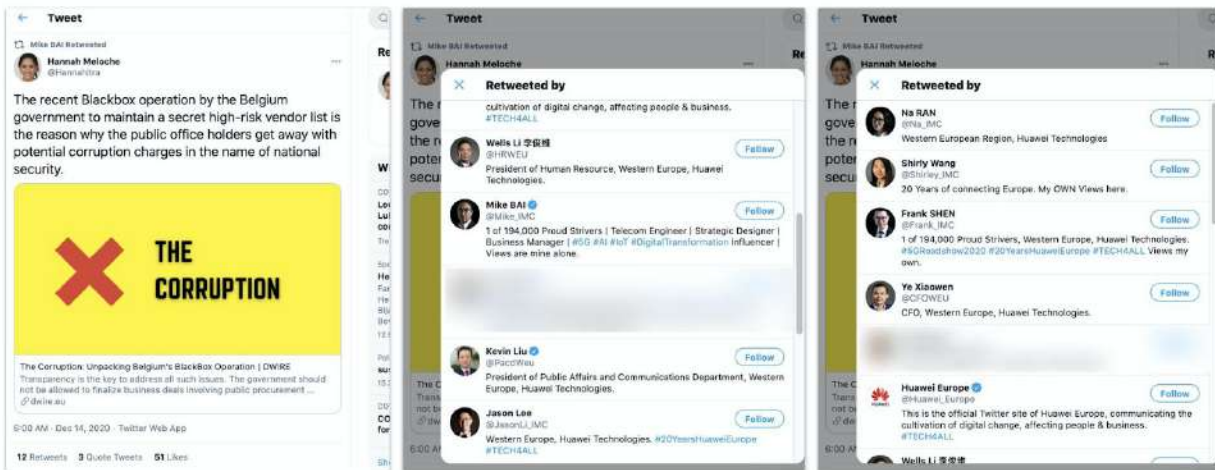


The Huawei Europe verified account sharing the "BlackBox" article as tweeted by four operation assets.

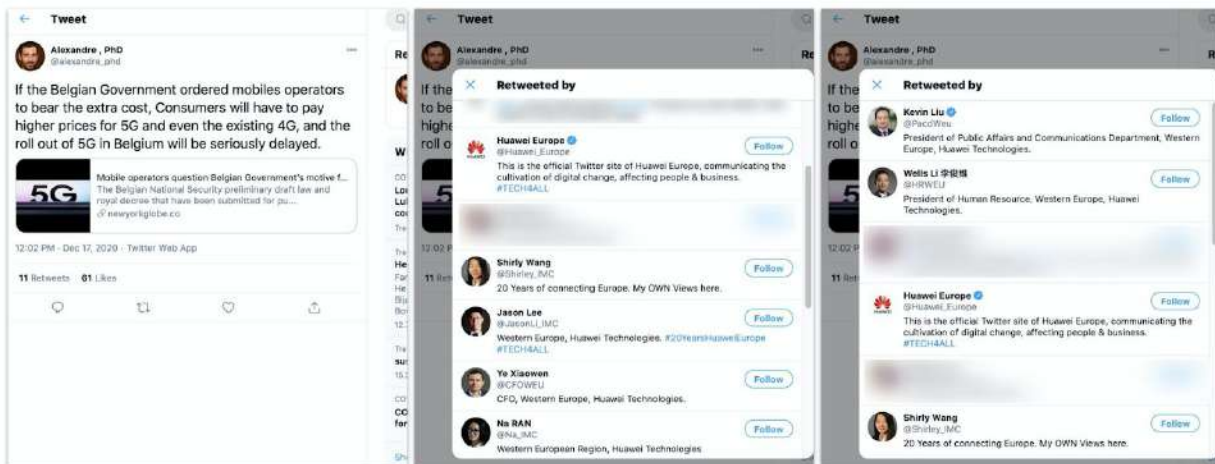


The Huawei Europe verified account retweeting three variants of the same article from different inauthentic accounts.

Other accounts that were attributed to senior figures in Huawei Western Europe also retweeted various accounts run by the operation. Two of them were verified: Kevin Liu, the president of the Public Affairs and Communication Department, and Mike Bai, whose Twitter bio did not name him, but who is identified by the [Huawei](#) website as president of Strategy Marketing. Further accounts attributed to employees of Huawei Western Europe included the Chief Financial Officer, the President of Human Resources, and the legal director.



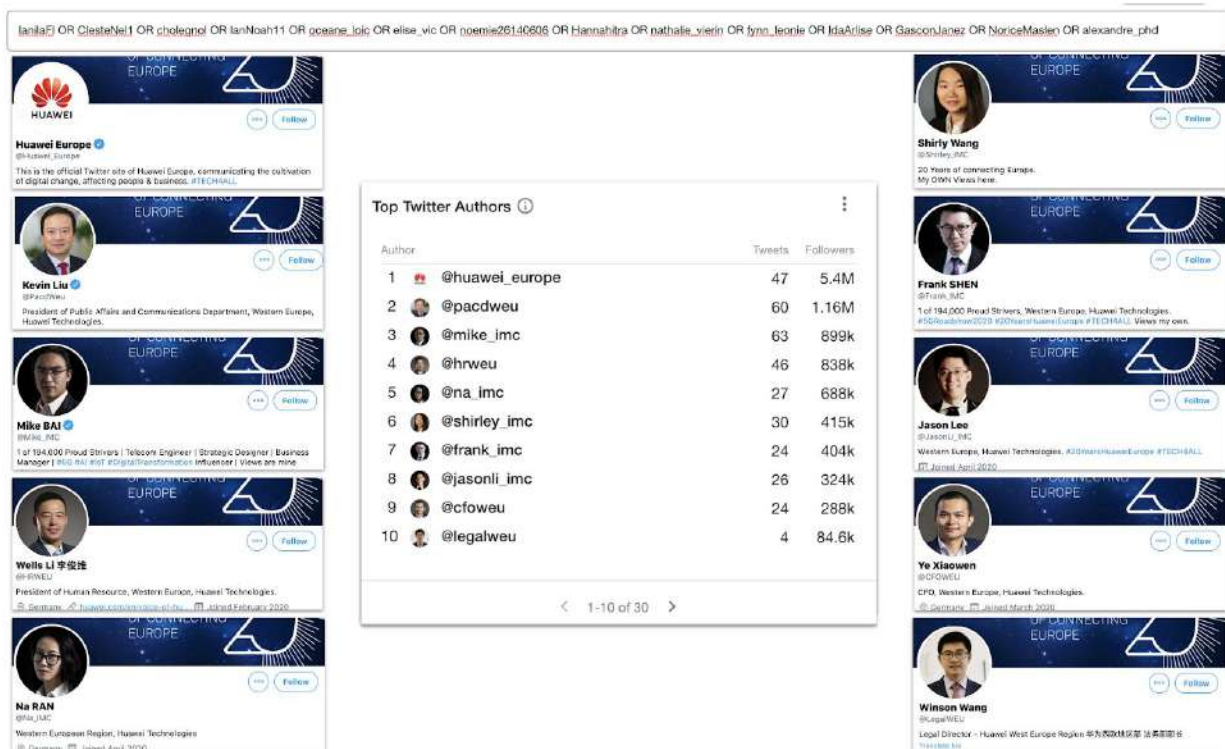
*Tweet by @hannahitra, together with its retweets; we have blurred out accounts that are not associated with Huawei, for clarity. Retweets are listed bottom to top, with the earliest at the bottom of the center image and the last ones on the top right.*



*Tweet by @alexandre\_phd, together with its retweets.*

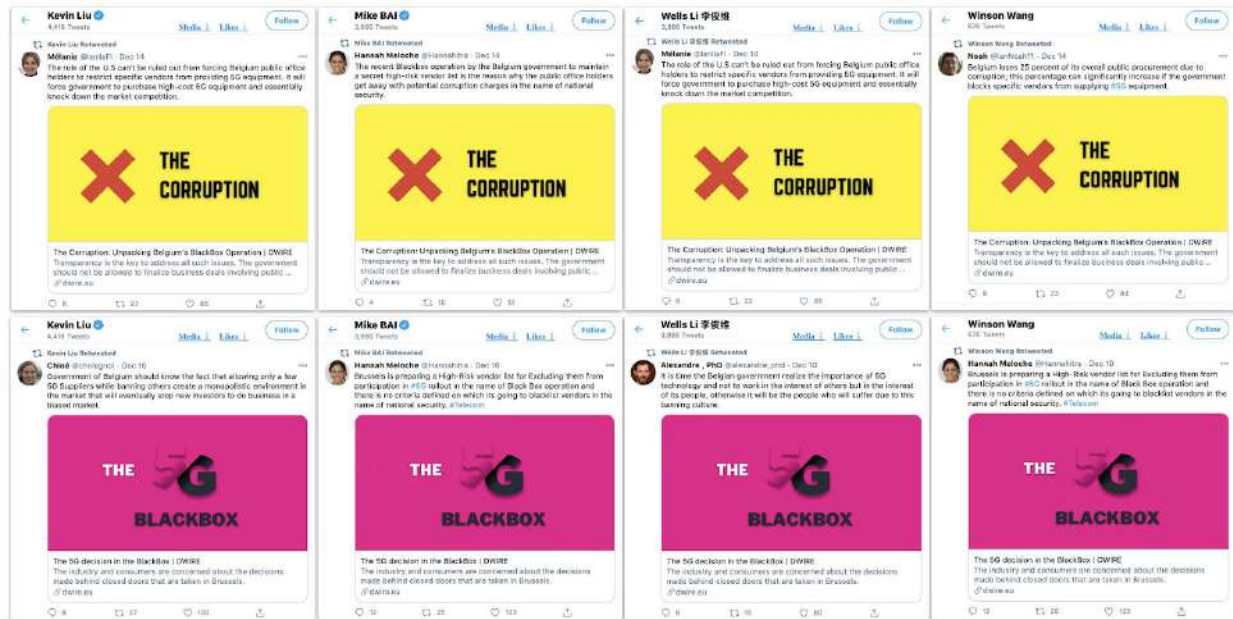
This retweeting by Huawei figures was a repeated occurrence. Graphika collected all mentions of any of the 14 fake accounts at any point in 2020, and analyzed which were the amplifiers with the highest followings, together with the number of times they mentioned or retweeted the fakes.

Overall, the Huawei officials were by far the most significant amplifiers of the fake accounts' output: they had the highest followings, and they typically mentioned the fake accounts dozens of times each.



Center and top, mentions of all the fake accounts, showing the top ten amplifiers sorted by following, together with the number of times they mentioned the fake accounts (column "Tweets"). Left and right, the profiles of those accounts.

This amplification by accounts attributed to Huawei executives also included the two articles that were posted on dwire.eu by fake personas, and that attacked Belgium for its "BlackBox" approach to 5G legislation.



Retweets of the articles on dwire.eu. Left to right, by [Kevin Liu](#), President of Public Affairs and Communications Department, Western Europe, Huawei Technologies; [Mike Bai](#), [President of Strategy Marketing](#), Western Europe, Huawei Technologies; [Wells Li](#), President of Human Resource, Western Europe, Huawei Technologies; and [Winson Wang](#), Legal Director, Huawei West Europe Region.



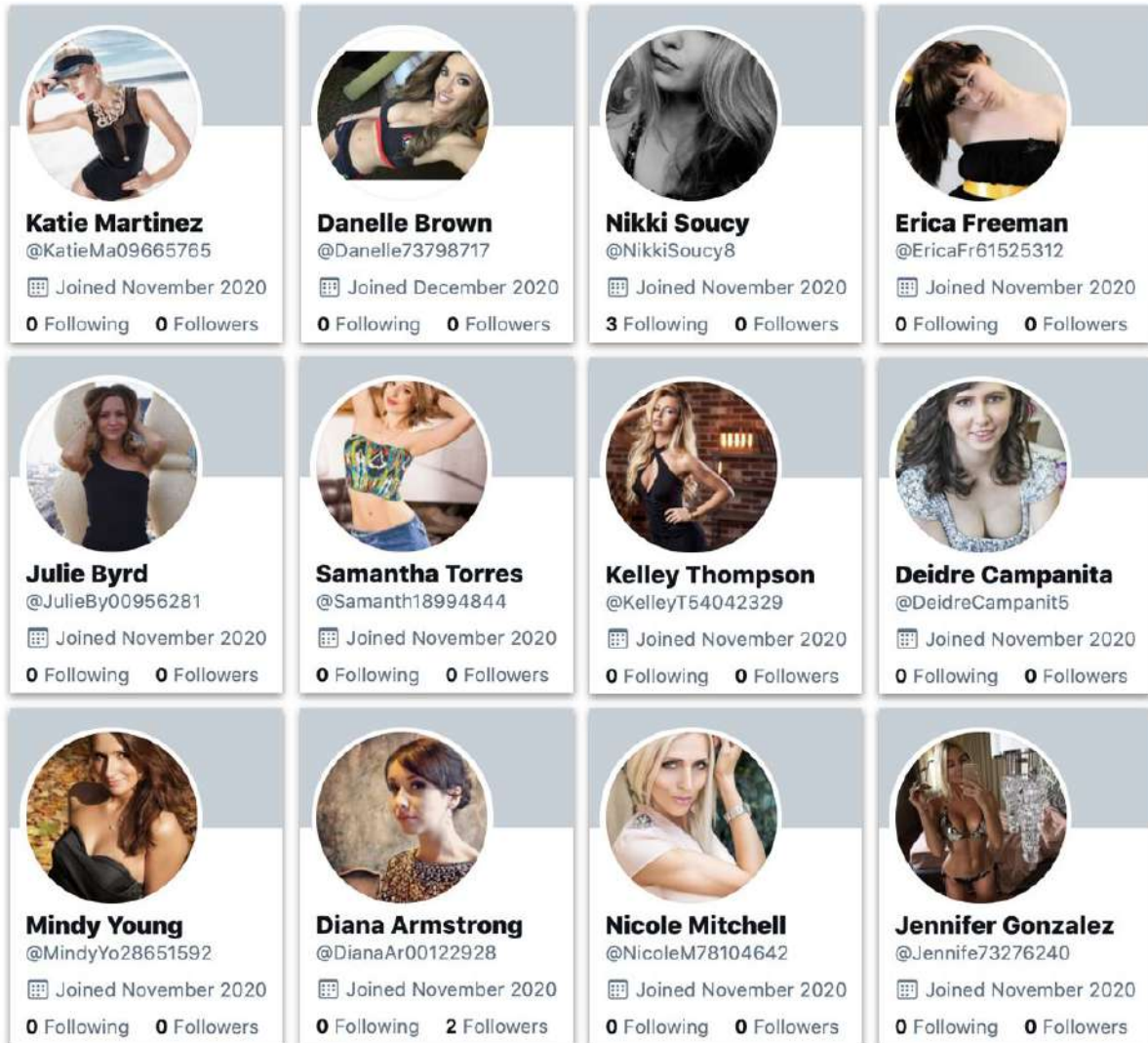
Retweets of the same articles. Left to right, by [Ye Xiaowen](#), CFO, Western Europe, Huawei Technologies; [Frank Shen](#), "1 of 194,000 Proud Strivers," Western Europe, Huawei Technologies; [Na Ran](#), Western European Region, Huawei Technologies; and [Jason Lee](#), Western Europe, Huawei Technologies.

# Shared Amplification

One other feature of this operation merits attention, and that is its amplification, on some posts, by a specific network of bots. These were created in batches and featured a “house style” of pictures of mainly Western women, and handles that consisted of seven letters followed by eight numbers.



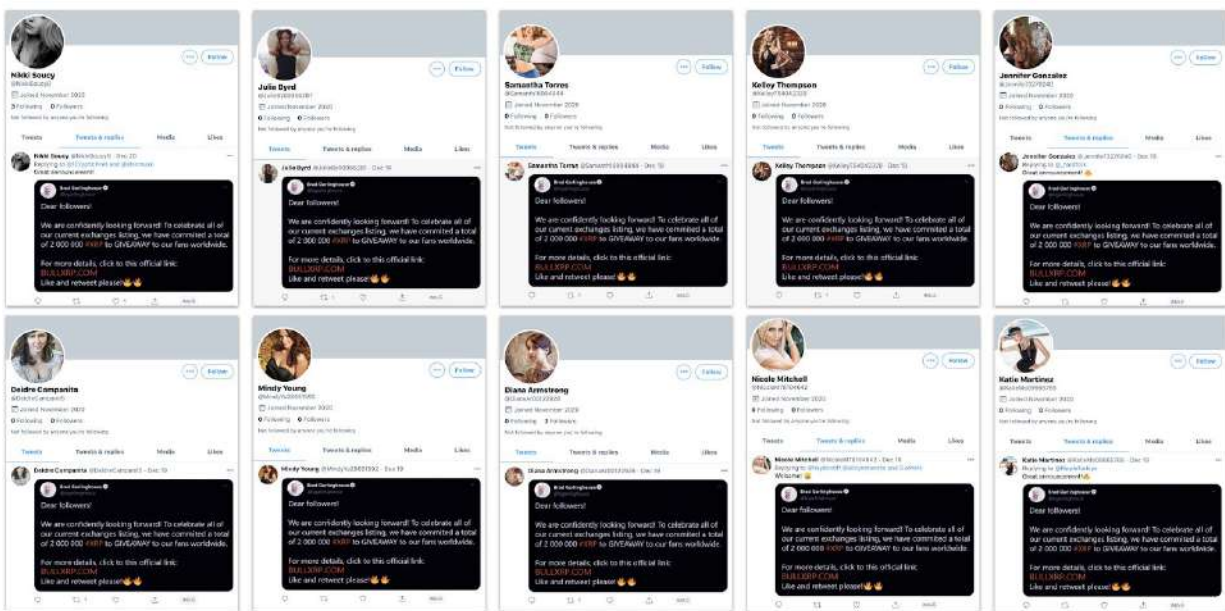
*Tweet by operation account @oceane\_loic, together with its retweets. Note that these included two subsets: accounts attributed to Huawei employees in Western Europe, and amplification bots.*



*The bots who retweeted the post by @oceane\_loic, above. Note the creation in November or December 2020, the standardized handles that most of them had, and the lack of followers.*

The bots in question were united by more than the style of their pictures (typically taken from Instagram influencers and other online sources) and default names: each one had only posted two or three tweets. One was a retweet of a post by the fake pro-Huawei operation. The others were screenshots - not retweets - of what purported to be a tweet by Brad Garlinghouse, the CEO of payments system Ripple, on December 15, offering to give away XRP, a [digital currency](#) issued by Ripple. No such tweet appears on Garlinghouse's timeline, but two weeks earlier he [shared](#) a tweet from Ripple warning against "scammers defrauding people with fake XRP giveaways." The likelihood is that this was another scam; it is important here because the vast majority of bots who amplified tweets by the fake pro-Huawei accounts also tweeted that screenshot as their only other post, sometimes with a few words of comment, such as "Thank you!" and an emoji.

It is statistically improbable that two unrelated botnets would both run bots that all tweeted, as one of their only posts, the same apparently fake image. We therefore conclude that the presence of that screenshot, when combined with the standardized handles and picture style, indicates members of the same botnet.

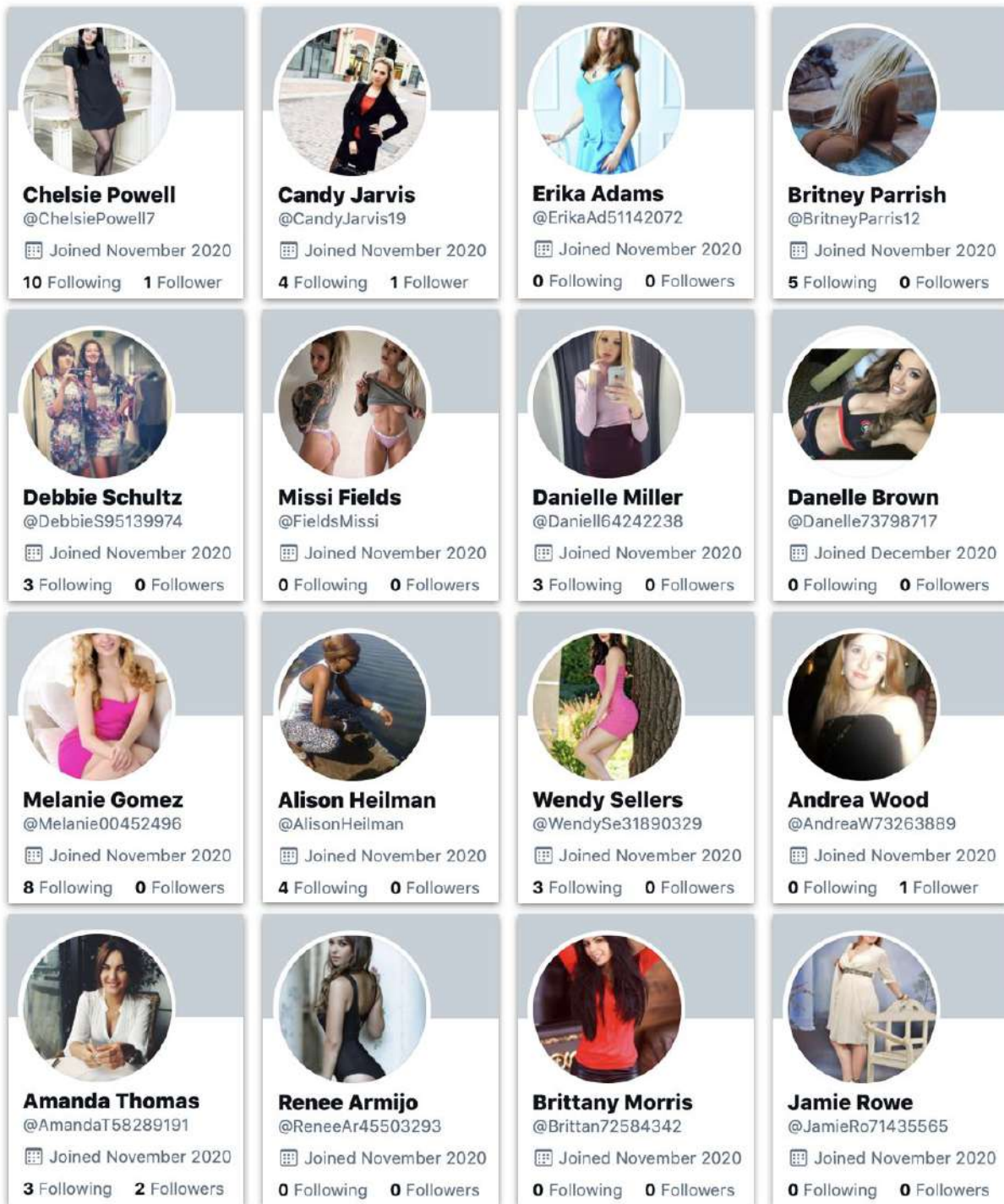


*Eight of the accounts that retweeted oceane\_loic, all tweeting the Garlinghouse screenshot.*

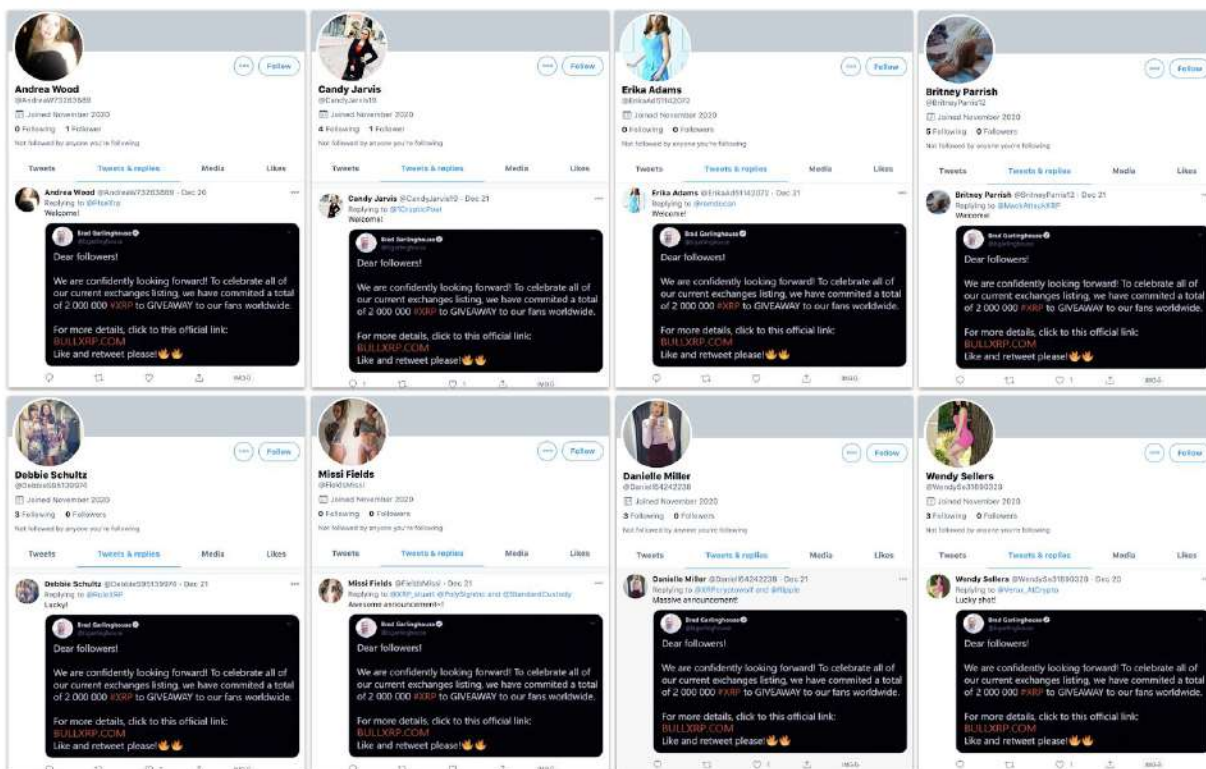
This is significant to our study because on several occasions, one or more members of this same network retweeted posts from the verified account of Huawei Europe. This should not be taken as implying that Huawei Europe was running the network of bots. Nor should it be taken as proof of who paid for them, if they were (as seems likely) a commercially available service: in theory, anyone could rent a network to provide extra amplification for Huawei. It does, however, provide further evidence that an as-yet unknown operation was using multiple techniques to support Huawei's messaging - both running fake accounts with GAN faces, and renting bots to provide subsidiary amplification.



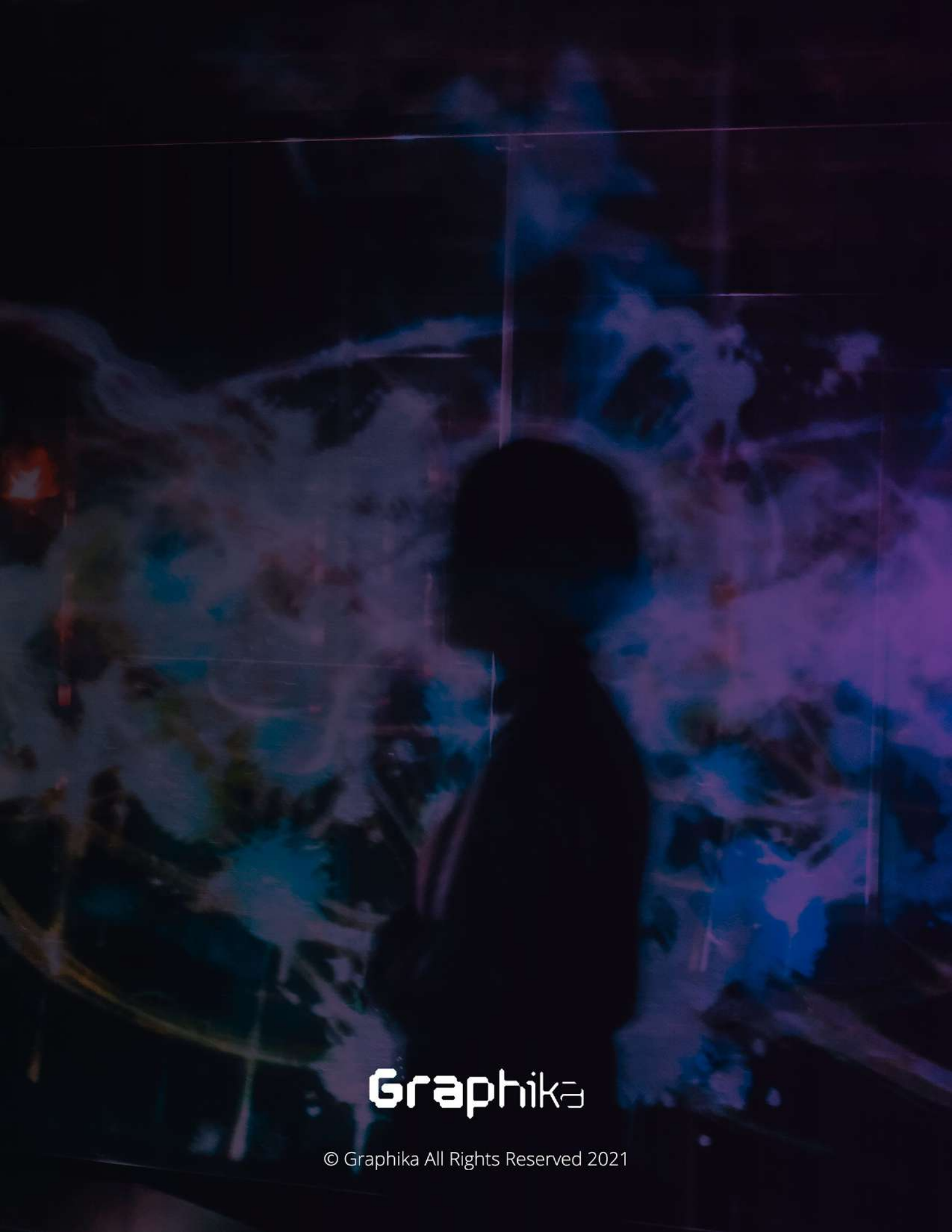
Tweet by Huawei Europe on December 20, together with its retweets: note the number of bots in the mix.



The profiles of the bots that retweeted Huawei Europe: as before, note the house style of photos and standardized handles, the creation dates in November, and the small or non-existent followings. Of all these accounts, only Danelle Brown also retweeted one of the Belgian fake accounts.



The same bots that retweeted Huawei, showing their posts of the Garlinghouse screenshot.



**Graphika**

© Graphika All Rights Reserved 2021