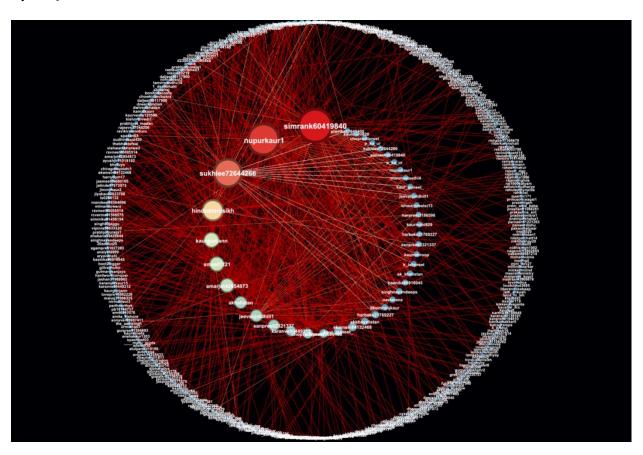


Analysis of the #RealSikh Influence Operation



Analysis of the #RealSikh Influence Operation

By Benjamin Strick



This report exposes a coordinated influence operation that uses fake personas on multiple social media platforms to promote narratives arguing that "real" Sikhs support the Indian government and Indian nationalism, and that advocates of Sikh autonomy and independence are extremist or terrorist.

The report identifies a core network of fake accounts that target other accounts supportive of Indian nationalism in order to spread and amplify the content and narratives generated by the core network. The report analyses the common profiles, content and tactics of the fake accounts which indicate their activity to be significantly coordinated.



Contents

Summary of findings	4
The network of fake accounts	4
Narratives promoted by the fake network	5
The political and information context	6
Assessing the impact of the fake accounts	7
Implications for India's political and social cohesion	8
Part one: Twitter RealSikh Network analysis	10
Network analysis	10
Profiles of the followers of the core network of fake accounts	14
Names of the fake accounts	17
Fake profile pictures	21
Repeat use of similar hashtags across the network	24
Use of English for all posts by fake accounts	28
Part two: Facebook and Instagram analysis	29
Part three: Frequently targeted narratives	34
Update: Actions by social media platforms	40
About the Centre for Information Resilience	41



Summary of findings

The network of fake accounts

A coordinated influence operation on Twitter, Facebook and Instagram is using fake personas acting as influencers within the Sikh community to discredit the push for Sikh independence, label Sikh political interests as extremist, stoke cultural tensions within India and international communities, and promote Indian Government content.

Our research identified a core network of 80 fake accounts that interacts with a much wider network of accounts, which appear to be authentic, to spread and amplify content generated by the core network.

The content produced by the network has endorsement from verified accounts and has breakouts on news and informational sites, where tweets from the core fake network are either linked to, or embedded in, posts.

While the core fake network maintained its presence on all three platforms through repeated posting and sharing of content produced by the other fake accounts, it gained significant momentum through its activity on Twitter, rather than Facebook or Instagram. For example, one tweet from one of the fake accounts on Twitter had more than 3,000 retweets and 16,000 likes, which was significantly more than any of the metrics identified on Facebook or Instagram.

That core network of fake accounts comprises of:

- 33 fake accounts on Twitter with a total of more than 84,000 followers.
- 29 fake accounts on Facebook with more than 80,000 combined 'friend'. Of the fake accounts, 22 were the same personas identified on Twitter, and used the same image, name, cover photo, and posted the same content.
- 18 fake accounts on Instagram, of which 14 were also copies of the personas on Facebook and 16 were copies of personas identified on Twitter.

Out of all of the accounts, 14 fake personas had accounts on all three platforms, using the exact same names, profile images, cover photos and same posts.

The fake accounts claim to be both "Real Sikhs" and "proud Indians". They use profile pictures stolen from celebrity social media accounts, use names common in Sikh communities to appear as legitimate members of the Sikh community, and are brazen in their calling out of whether someone is a "Real Sikh" or a "fake Sikh". The fake accounts do not show signs of automation, but rather appear to be human-operated, acting as 'sock puppet' accounts with the same personas replicated over multiple platforms and repeating the same content. The core network is supported by a large network of authentic accounts which primarily identify as Hindu nationalists.



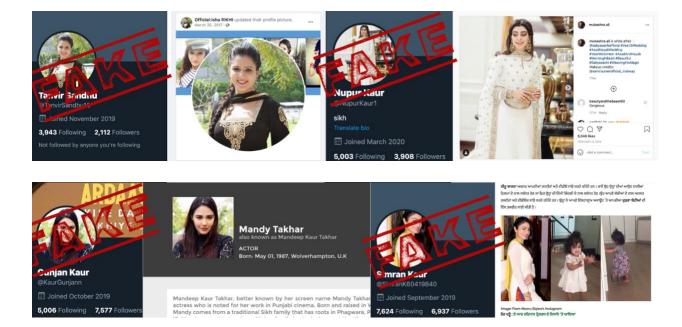


Image 1: Examples of the core fake accounts using images from authentic accounts

Narratives promoted by the fake network

The accounts target their content at numerous issues, but primarily use the Khalistan movement to claim any notion of Sikh independence is extremist and terrorist related, that Pakistan is fuelling Sikh independence movements in India, and that western countries (namely the UK, US and Canada) are harbouring Sikh terrorist groups. The network uses hashtags related to Khalistan and terrorism when commenting on significant issues in India and abroad to target Sikh independence, farmers' protests, activists and more.

Some of the fake network's messaging included statements calling for action such as Indian "Nationalists shouldn't remain watching silently" and that they "need to counter & expose them I the Khalistani movement for Sikh independence]" to "save India" from "Pakistan, Canada, UK, and US".

The network increased its activity since the commencement of the farmers' protests in India which have been ongoing since late 2020. Both the farmers' protests and the Khalistan independence movement have been the two most frequently targeted subjects of the core network of fake accounts.



The political and information context

The farmers' protests have been an ongoing protest movement in response to legislation relating to farming passed by the Indian Government in 2020. In November 2021, the Indian Government <u>announced the repeal of the laws</u> amidst <u>mounting pressure</u> and scrutiny over the laws. The laws were contested by farmer unions claiming they were <u>'anti-farmer'</u> as the laws put farmers 'in danger of becoming captive to companies' and that farmers would be left worse off.

Numerous media outlets claimed the farmers' protests were <u>hijacked</u> or <u>infiltrated</u> by 'extremist' groups. These were fuelled by <u>claims</u> from Indian politicians such as National General Secretary of the Bharatiya Janata Party (BJP) Dushyant Kumar Gautam that there were links between the farmers and the pro-independence Khalistan movement. However, some farmers claimed the BJP's statements about extremism were <u>'government propaganda'</u> to delegitimise the movement, label farmers as <u>terrorists</u>, and scare people into supporting the government to crackdown on the demonstrations.

The core network of fake accounts promotes content that labels the Khalistan movement as extremist. The Khalistan movement refers to a campaign for the <u>creation of a sovereign Sikh state</u> (called Khalistan) in Punjab, India, which became highly politicised following a military campaign in 1984 called 'Operation Bluestar'. In that campaign, the Indian military stormed the Golden Temple in Amritsar in an attempt to remove Sikh militants. <u>Human rights' researchers reported</u> that thousands were killed, most of them civilians. This led to outrage and further calls for an independent state. <u>Human rights' researchers documented</u> increasingly brutal methods used by security forces in the crackdown on advocates of independence following Operation Bluestar, including "arbitrary arrests, torture, prolonged detention without trial, disappearances and summary killings of civilians and suspected militants".

In the content produced by the fake network, many of the memes and text are promoting the narrative that the Khalistani movement was 'trying to hijack the farmers protest' which is an attempt to delegitimise the farmers movement and shift the debate away from the farmer laws and into what the accounts claim is an issue about "terrorism" and "Khalistan".

The use of social media to influence narratives in India has been an ongoing issue. In 2019 Facebook removed more than 600 pages and accounts that were engaged in 'coordinated inauthentic behaviour' and were 'linked to individuals associated with an IT Cell of the Indian National Congress (INC)'. On Twitter, numerous inauthentic campaigns have been exposed such as mass manipulation during elections using Google Docs to spread messaging supportive of the Indian Government. There have also been inauthentic operations targeting the EU and UN, fake news sites, fake fact checking sites promoting the Indian Government and discrediting its opponents, pro-government actors amplifying violence against protesting farmers and claims of state-linked trolling campaigns.

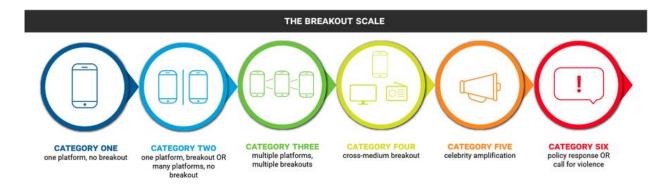


While there appears to be significant efforts to manipulate the digital information space, there are also signs of government-backed censorship and restrictions on media and those critical of the government. For example, in July 2021 Twitter issued a transparency report indicating that India was the 'single largest source of government information requests', accounting for 25% of the global volume. Twitter also removed numerous tweets critical of the Indian Government's handling of the coronavirus pandemic, at the request of the Indian Government. The platform has also been served with blocking orders by the Indian Government.

Assessing the impact of the fake accounts

Assessing the impact of the network, and others like it, is difficult given the nature of post-review metrics. However, one proven method to evaluate the impact of the network was summarised in a report detailing a <u>'Breakout Scale'</u> by Ben Nimmo, Global Influence Operations Threat Intelligence lead at Facebook parent company Meta.

The Breakout Scale is a model that addresses the challenge of assessing the impact of influence operations and disinformation. It divides influence operations into six categories indicative of 'whether they remain on one platform or travel across multiple platforms (including traditional media and policy debates), and whether they remain in one community or spread through many communities'.



The core network of fake accounts appears to have gained significant traction on Twitter with breakouts into news and information sites. In some cases, this would either be links in the articles to the Twitter accounts, or in other cases it was embedded tweets within news posts. These breakouts appear to be organic in nature.

The network is also present on Facebook and Instagram. We consider this network to fall within Category three of the breakout scale. Category three specifically looks at the network's presence on multiple platforms with multiple breakouts.



In terms of the organic interactions with the network, there appears to be significant uptake primarily on Twitter in terms of retweets and likes. There appears to be high levels of amplification of some tweets (with tweets like this getting more than 16k likes). We also identified a number of interactions and endorsements from the verified accounts of public figures, humanitarians and personalities. For example: here, here, here, here and here.

We also identified the spread, or breakout, of the network's content to other websites through what appears to have been organic sharing (the pages and accounts sharing them do not appear to be part of the network). For example, the fake network's content was present as embedded links within articles on commentary and news blog sites including: Latestly, Voice of India World, Asianetnews, IndiaTV, NewsCom. This is likely to have strengthened the legitimacy of the fake network's content and increased its exposure and is a clear example of a breakout from the network's presence on social media platforms to off-platform sites.

Implications for India's political and social cohesion

Our research has exposed an inauthentic influence operation that is using fake accounts in a coordinated manner across multiple social media platforms to promote narratives and content arguing that Sikh independence is not compatible with either the values of a "real" Sikh, Indian national interests, or support for the current government and that anyone advocating independence is an extremist or even a terrorist.

The core of the network are accounts positioning themselves as true Sikhs, whilst their content is amplified by accounts self-identifying as Indian nationalists. This suggests the influence operation may be targeting audiences within both Sikh and Hindu communities. The profiles of the fake accounts, their adoption of common Sikh names, their use of similar if not identical spam hashtags and content, and our analysis of their interactions with other Twitter users, suggests their activity is coordinated.

The basis of this report is publicly available information. This enables identification of narratives, tactics, and techniques, but precludes attribution of responsibility for the fake network and its activity to specific actors. Conclusive attribution requires a number of points, one of which is access to data held by social media companies which is not accessible to external researchers such as the Centre for Information Resilience.

However, application of the Breakout Scale, explained above, suggests the fake network's impact is important given its targeting of multiple platforms, endorsement by legitimate Twitter accounts with large followings, and further amplification through breakouts on news and blog sites. Some tweets by the fake network which targeted the UK and Canada as homes of the Khalistani movement have received more than 16,000 likes, indicating significant traction on the platform.



Continuation or expansion of the network's activity therefore risks reducing cohesion within the Sikh community, weakening trust and understanding between India's different religious communities, and increasing social divisions that could undermine the stability of one of the world's largest and most diverse democracies. The network's advocacy that supporters of Sikh independence are extremist or terrorist, and that Indian nationalists must take action against them, may contribute to an environment in which some actors consider intimidation of, or violence towards, the Sikh community as legitimate.



Part one: Twitter RealSikh Network analysis

This section of the report is focused on how content generated by the fake network has spread via Twitter, specifically how it used the platform to spread and amplify its narratives opposing Sikh independence and supporting Indian nationalism.

Through our research, we identified a core group of 33 fake accounts. There were a number of traits we noticed that were unique to these accounts, which assisted in the identification of the rest of the accounts in the network.

The common characteristics of the accounts were:

- 1. All had more than 2,000 followers, with the exception of one account that appeared to be new in the network. Accounts with more activity had more than 6,000 followers each.
- 2. All of the accounts appear to follow as many accounts as they have following them, if not more.
- 3. The followers of the accounts, as well as the accounts themselves, appear to be humanoperated and not automated.
- 4. All of the accounts use names that are very clearly Sikh names in order to be seen as Sikh and as part of the community.
- 5. Almost all of the fake accounts use profile pictures of celebrities
- 6. All of the accounts used repetitive hashtags with the word 'Khalistani' in them, for example #Khalistanis, #RealSikhsAgainstKhalistan, #SikhsRejectKhalistan and #ShameOnKhalistanis.

These common characteristics provide an insight into how content and narratives promoted by the network are spread and amplified. The following paragraphs provide a more detailed analysis of those characteristics.

Network analysis

We collected the data of 398 accounts that had liked, retweeted or commented on tweets that used the hashtags #RealSikhsAgainstKhalistan, #SikhsRejectKhalistan and #RealSikhs. These were three hashtags that appeared to be commonly used in the network, particularly by accounts with larger numbers of followers.

This data was collected by querying Twitter using the Twitter Search API to obtain recent tweets matching the queried hashtag. This was done in order to track the spread of the conversation relating to each hashtag, rather than the tweets alone, in order to then identify amplifier accounts and to assess the impact of the network.

We created a visualisation of this network, below, with the nodes (accounts) appearing as circles, and interactions between accounts such as likes, retweets and comments, represented as lines between the nodes.



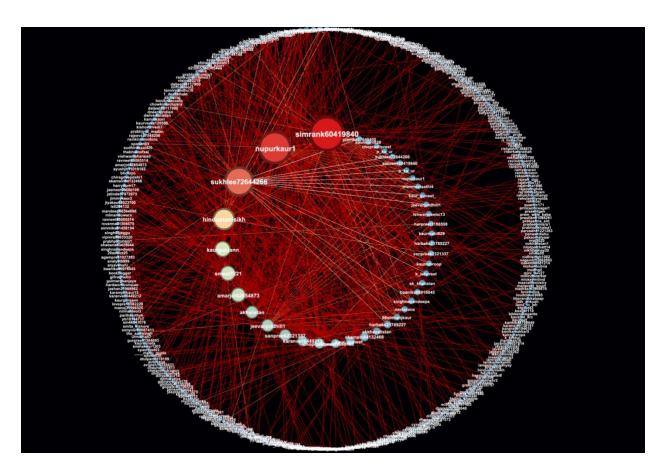


Image 2: Visualisation of interactions between core fake accounts and other Twitter users.

The visualisation uses a dual circle layout function in Gephi to identify the accounts that have more prominence within the network. In the inner circle the nodes and their names appear larger to illustrate the higher number of interactions (likes, comments and retweets) between the specific posts that used one of the "Khalistani" hashtags and other accounts.

Visualisations based on the number of interactions are helpful in identifying not only the accounts that have more traction – in this case the core network of 80 fake accounts – but also the supporters of those core accounts who spread and amplify their content.

It is also helpful as a visual aid to highlight the significance of how a small number of well-curated 'sock puppet' accounts that post regularly and target an existing genre of culture online, can influence public opinions and amplify specific talking points to such a wide audience.



For example, the most popular account in this dataset is @simrank60419840. In the image below, we can see through the account's connections, that there is prominent support from both the outer circle (the wider Twitter community), as well as from the inner circle (the core fake accounts), especially on the right side of the inner circle which are ranked anticlockwise in terms of prominence.

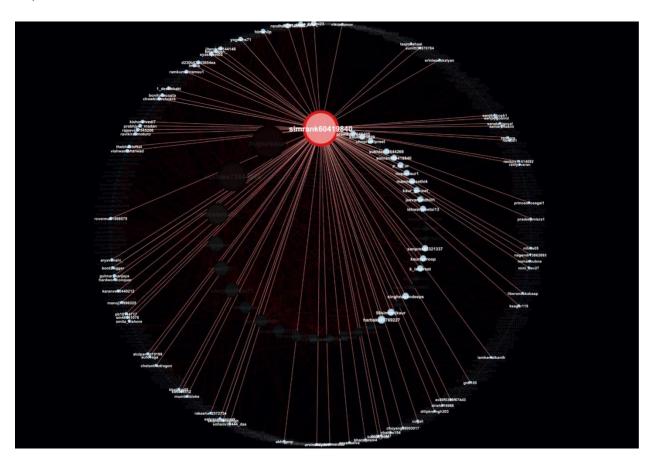
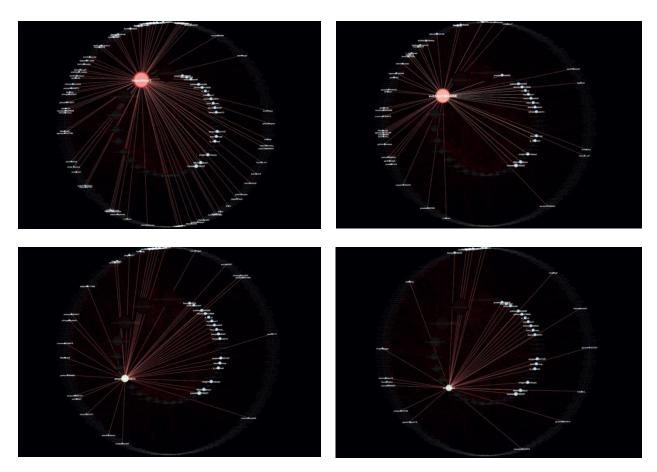


Image 3: Network analysis focused on Twitter account @simrank60419840.



The same pattern can be identified in other larger accounts, such as @nupurkaur1, @sukhlee72644266, amarjot42854873 and @akhalistan.



While an overview of a sample of the network's activity is useful in capturing possible size, spread and how it amplifies its content, it is important to observe the granular detail of individual accounts to identify their tactics, techniques and procedures in manipulating the information space.



Profiles of the followers of the core network of fake accounts

Many of the accounts appeared to have large numbers of followers, and were following just as many accounts, if not more. This may indicate that there has been a considerable effort spent to build up these accounts by following those that fall within the target audience or intended demographic of this influence operation.

Below are some of the accounts in the network to indicate the follower/following ratio.













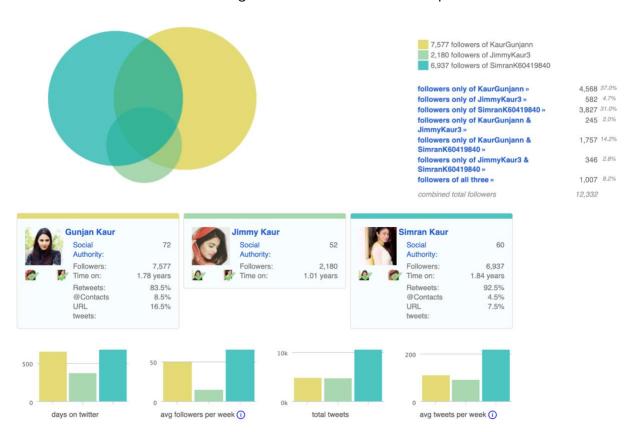




Many of the accounts in the network appear to have overlaps with other fake accounts in terms of both the people they follow as well as the people they have following them. For example, in an assessment of accounts @kaurgunjann, @jimmykaur3 and @simrank60419840 there are 1,042 accounts that are followed by all three. There are also 1,007 accounts that follow all three accounts. These following accounts appear to be authentic human-operated, and do not appear to be using methods of automation that have been seen in other social media amplification networks.



Below is a visualisation made through Followerwonk of the overlap of the accounts.



While the overlap of followers across accounts does not indicate anything specific on its own, it should be taken in context with the analysis of other publicly available information. For example, we also assessed the biography field of the Twitter accounts that were following five of the most prominent fake accounts as the biographies of the followers frequently included the words "proud", "Indian", "Hindu" and "nationalist".



We looked in detail at the biographies of the followers of five accounts from the core fake network: <code>@KaurGunjann</code>, <code>@JimmyKaur3</code>, <code>@Jasmeeto9660105</code>, <code>@Gurpree91384693</code> and <code>@SimranK60419840</code>. Word-clouds were created to indicate the most commonly used words in the followers' biographies. Those word-clouds can be seen below.

Bio word cloud of KaurGunjann's followers

To help make sense of the "biography" field of each Twitter user, we've assembled this word cloud which shows you the most frequently occurring words.

proud — indian — hindu — love — nationalist — india — follow — jai — first — rts

- nation - life - endorsement - endorsements - engineer - personal - fan - views - lover - social - back - student - 第 - only - world

Bio word cloud of JimmyKaur3's followers

To help make sense of the "biography" field of each Twitter user, we've assembled this word cloud which shows you the most frequently occurring words.

proud — indian — hindu — india — love — nationalist — follow — jai — first — nation —

endorsement - life - back - lover - fan - engineer - student - rts - hind - \(\frac{1}{2}\)f - world - sikh - endorsements - personal - people

Bio word cloud of Jasmeet09660105's followers

To help make sense of the "biography" field of each Twitter user, we've assembled this word cloud which shows you the most frequently occuring words.

proud - indian - hindu - love - india - jai - follow - nationalist - endorsement -

life - first - lover - nation - rts - live - engineer - back - sikh - support - भारत - bharat - endorsements - views - social - भार

Bio word cloud of Gurpree91384693's followers

To help make sense of the "biography" field of each Twitter user, we've assembled this word cloud which shows you the most frequently occurring words.

proud - indian - hindu - follow - india - love - nationalist - first - jai -

nation - life - endorsement - fan - back - sikh - engineer - endorsements - personal - rts - lover - world - नहीं - religion - country - student

Bio word cloud of SimranK60419840's followers

To help make sense of the "biography" field of each Twitter user, we've assembled this word cloud which shows you the most frequently occuring words.

proud - indian - hindu - love - nationalist - india - follow - jai - first -

 $endorsement-nation-rts-life-endorsements-{\it fan-engineer-personal-lover-bharat-back-{\it sh-upf-right-views-world}}$



The word-clouds indicate that there appears to be strong similarities in the biographies of many of the followers of the accounts and the overlap of words such as "proud", "Hindu" and "nationalist". This may be explained by the pre-existence on Twitter of a number of accounts whose owners are supportive of Indian nationalism and who have chosen to follow discussions of Sikh-related issues on Twitter by tracking the hashtags aimed at the Khalistani movement. This interpretation would also explain the existence of overlapping followers of the fake accounts, and overlaps in who they follow, that was analysed above.

The connection between these – likely authentic – accounts and the core network of fake accounts may be due to the core accounts having identified people on Twitter already posting pro-government and nationalist content and having then connected with those people in order to utilise them as a body of nationalist supporters that will amplify the core network's tweets.

Names of the fake accounts

Examining a list of 33 accounts on Twitter we identified in our research, 18 of them use the surname "Kaur". Kaur is a common surname for Sikh women as it means 'princess'.

Other surnames that appeared in the core network of fake accounts were Dahiya, Singh and Sandhu, all of which are also common Sikh surnames.

The use of these names, along with the fake profile pictures and the 'proud to be Sikh' slogans often seen tweeted from the accounts, appears to indicate that these accounts wanted to be seen as Sikhs in order for their narratives on Sikh agendas to be influential.

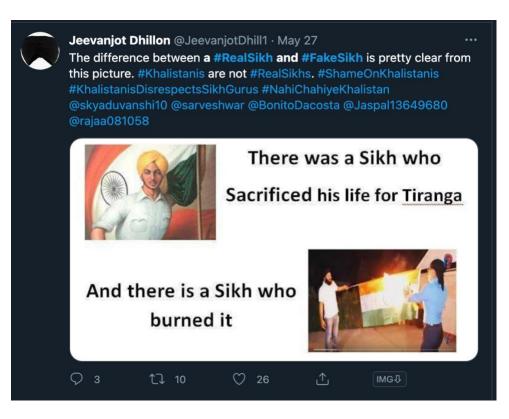
Tweets from the fake accounts included messaging intended to convey their legitimacy as Sikhs through tweets about "RealSikhs" and "FakeSikhs", before advocating the positions that Sikh's should take on political issues such as independence. Below are examples of how this was done. These posts were identified by searching the phrase "#RealSikh and a #FakeSikh".





















Fake profile pictures

Many of the fake accounts in the core network identified in this research used images of celebrities as their profile pictures. While an initial image reverse search did not reveal the same images immediately, after repeated searches of similar looking people we were able to identify the exact same images used by the celebrities and confirm that the image was indeed fake.

This also indicates an attempt to make the search for the profile images slightly more difficult than just through an image reverse search. The majority of core accounts used images that were not immediately present after conducting an image reverse search on Google Image reverse search or Yandex image reverse search. Some of the accounts had either used images that were on social media platforms such as Instagram, that did not index on Google.

One of the accounts with more than 6,000 followers is Simraun Kaur, who uses the Twitter handle @SimranK60419840. Simraun's profile image is actually that of Neeru Bajwa, a Canadian actress who started her career in Bollywood films.

Another account, Nupur Kaur, who also identifies as Sikh through her biography, is actually the photo of the sister of Mubashra Aslam, seen here in a dress.

Tanvir Sandhu, is using the image of actress **Isha Rikhi**.







Gunjan Kaur is using the image of actress Mandy Takhar.





Mandy comes from a traditional Sikh family that has roots in Phagwara, P

Armajot Kaur uses an image of Nimrat Khaira.







Jimmy Kaur uses an image of Punjabi actress Wamiga Gabbi.





While the use of fake profile pictures may appear to be deceptive, it does not, on its own, mean that there is inauthentic activity. But rather, in looking at the whole, it appears that the use of fake profile pictures in this network may indicate the intention to conceal the identity of the real actor/s behind the accounts and represent themselves as something they are not.



Repeat use of similar hashtags across the network

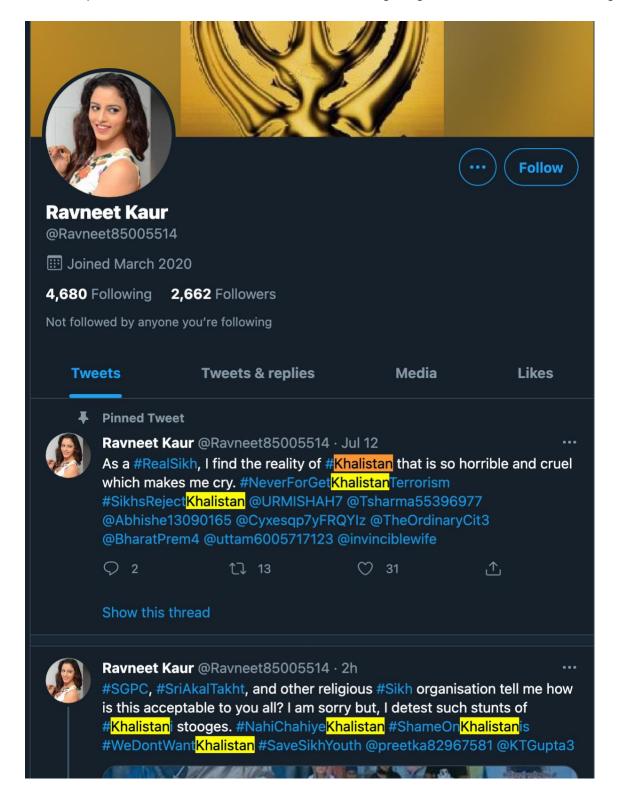
There are signs that the core network of fake accounts is coordinated through the use of the same, or very similar hashtags. These are often specific to the narratives which will be discussed more below.

While the use of the hashtags #RealSikh and #FakeSikh have already been referenced above, their usage has been common in the network whenever there is criticism of a Sikh issue – this has been especially the case around the issue of the Khalistani movement, with many tweets claiming that #FakeSikhs support the Khalistani movement, as seen below.





Many of the accounts identified in the core network use similar keywords in their hashtags in different variations, many of which are hashtags unique to this network and not used by others. For example, this can be seen in the account below targeting the Khalistan word in the tags.





By looking at one of the longer hashtags used by 'Ravneet Kaur' such as #NeverForgetKhalistanTerrorism, we can identify further amplification of this hashtag which crosses over with many of the accounts identified in this report.















Some hashtags targeting the Khalistan movement appear to have gone more viral than others, such as the one below (archived here) which received more than 16,000 likes and 3,000 retweets.



The accounts also posted in a similar manner by tagging other accounts in threads, just like using the hashtags. This might be to gain traction in the original tweet in the hopes of strong amplification levels, or to signify to nationalist or supporting accounts that a new post has been made by the influencer.



There have been numerous topics, such as suggesting foreign harbouring of Khalistan in Canada and the UK as well as targeting activists by mixing in several unique hashtags. An example of this can be seen below.





Use of English for all posts by fake accounts

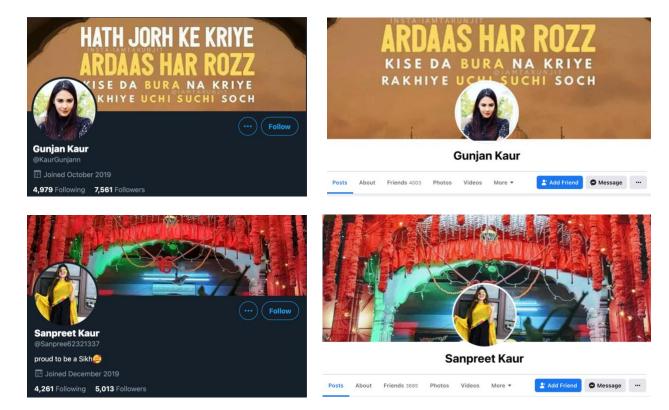
Much of the content seen on Twitter, as well as the other platforms, was posted in English. While the research was conducted in English, reviews of the main influencer accounts identified very little content posted in Punjabi. This may either be due to the targeted audience of the network being non-language specific (using English rather than specifically Punjabi or Hindi), or because the people operating the Sikh influencer accounts are not able to write sufficient text in Punjabi.



Part two: Facebook and Instagram analysis

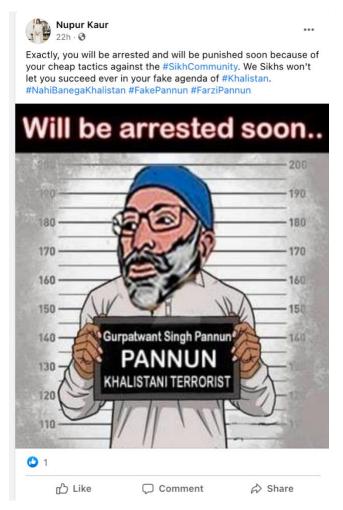
The fake Twitter accounts appear to use similar names in a standard operating persona, and after a search on Facebook, our research identified almost all of the Twitter accounts had the same personas on Facebook.

Many of the fake accounts used the same profile picture, and in many cases the same cover photo to standardise the personas across platforms.





It was evident throughout the research that the individual personas cross-posted content and memes and used the same hashtags in their posts on both Twitter and Facebook.









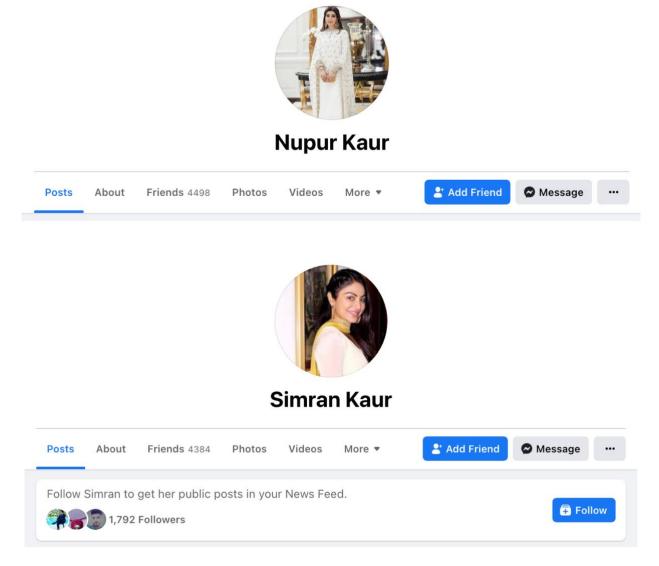








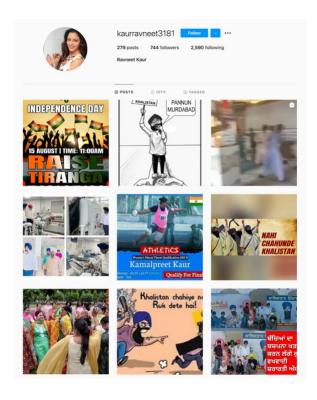
The personas on Facebook also had the similar hallmark of the accounts on Twitter by appearing to have significant numbers of followers and using the same fake profile pictures which were stolen from celebrities.

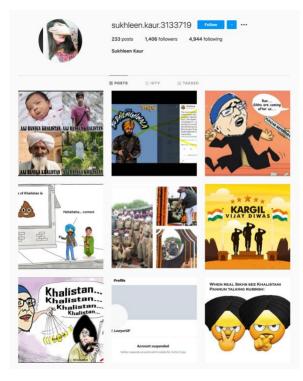


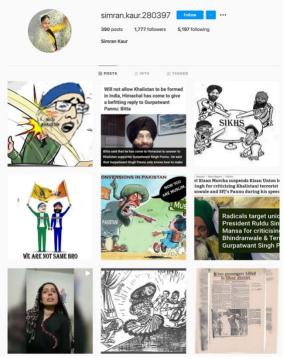
Due to Facebook's search restrictions and privacy, we were not able to assess the authenticity of all of the followers. However, many of the accounts we did look at appeared to be authentic users of the platform.

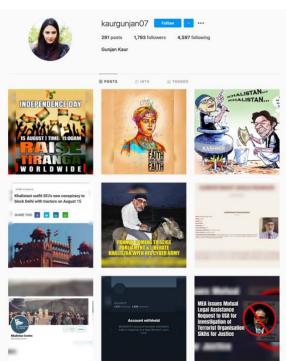


Many of the core fake accounts on Twitter and Facebook were also replicated on Instagram with the same images and names and posted extremely similar content, however one difference was the number of followers they had. Unlike the Twitter and Facebook accounts, however, the Instagram accounts were following a higher number of accounts than they had followers.











Part three: Frequently targeted narratives

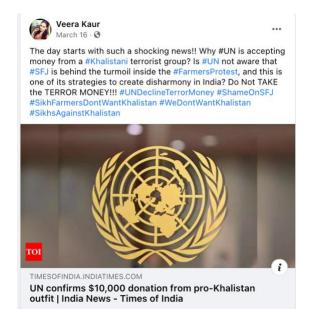
Our research identified a number of narratives currently being promoted by the core network of fake accounts. While these narratives shift across different subjects, there appears to be a consistent theme of using the Khalistani movement as a way to inflame topics.

One of the narratives identified in the research was targeting the farmers' protests. The fake network has repeatedly used messages claiming that 'Khalistani terrorists' hijacked the farmers' protests. This message, conveyed through memes and text, is likely an attempt to delegitimise the farmers' movement and shift the debate away from the farmer laws and into what the accounts claim is an issue about "terrorism" and "Khalistan".

The platforms suspended these accounts from the platforms off the back of this research, which was just days prior to the announcement of the <u>repeal of the farm laws</u> in November 2021.











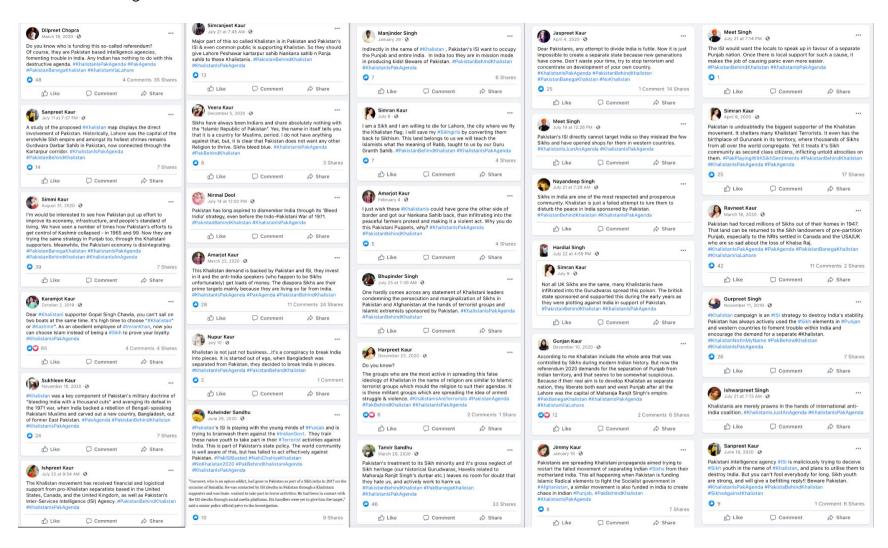
One post in the fake network attempted to <u>rally nationalists to 'save India'</u> in that Indian "Nationalists shouldn't remain watching silently" and that they "need to counter & expose them" to "save India" from "Pakistan, Canada, UK, and US".



Another narrative which can be seen from the screenshots in the above posts is that foreign countries are providing a home to the Khalistani movement and thus threatening India. There are numerous references to the UK, Canada and the US in this context – which might indicate an intention to convince either Sikhs in those countries that the US, UK and Canada are interfering in India, or for Sikhs in India that those countries are trying to interfere.

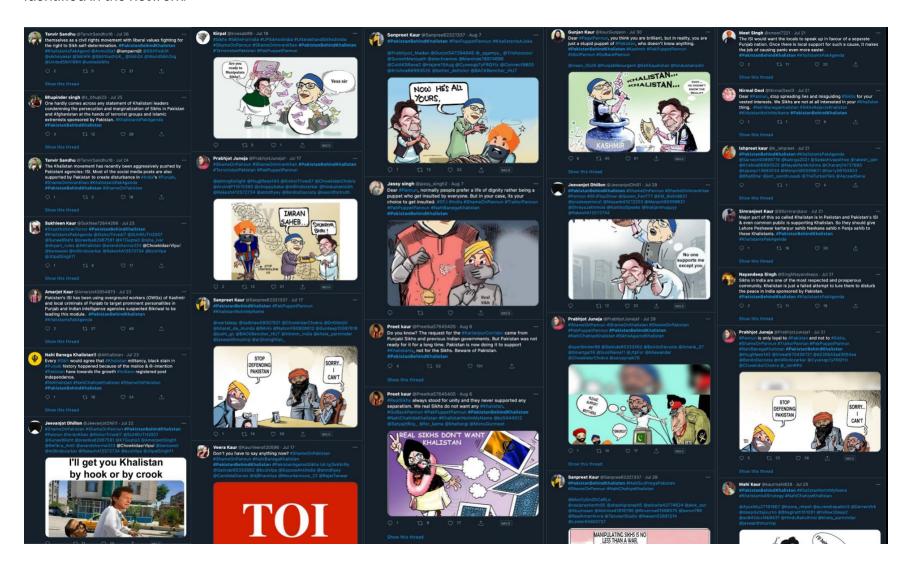


Pakistan also features heavily in claims of funding and support to the Khalistan movement. This can be seen in screenshots below which were identified on Facebook by searching hashtags promoted by the network such as: #PakistanBehindKhalistan, #KhalistanIsPakAgenda and #PakBehindKhalistan.





Very similar messaging, with the use of cartoon memes, appeared on Twitter under the same hashtags by many of the same personas identified in the network.





One fake account (@SimranK60419840) appears to have a significant reach in many of its posts about western countries harbouring the Khalistan movement. In one <u>tweet</u> there were interactions of more than 16,000 likes, while many other tweets about the issue also appear to have significant impact and spread.









While there appears to be significant links and complementarities between the fake network's messaging concerning the Khalistani issue, foreign interference and the farmers' protests, many of the accounts have also posted content highly supportive of the Indian Government, specifically the Indian Defence Force, and praising of past battles and officers. One of the common topics of praise for the army was about the Kargil War in 1999 where India regained possession of an area from Pakistan through armed conflict.















Update: Actions by social media platforms

Prior to publication this report was shared with teams from Twitter and Meta that specialise in threat intelligence and influence operations.

The platforms identified in this report where the fake network was visible have policies governing their use, specifically around platform manipulation and spam (as seen on <u>Twitter</u>) and inauthentic behaviour (as seen on <u>Meta</u>).

After reviewing the findings of this report, the accounts identified and analysed in this research have subsequently been suspended for violations of policies prohibiting platform manipulation and inauthentic behaviour.



About the Centre for Information Resilience

The Centre for Information Resilience (CIR) is an independent, non-profit social enterprise dedicated to identifying, countering and exposing influence operations.

The CIR, supported by an advisory board of experts, works to raise awareness among policymakers, journalists and the public of the risks posed by influence operations by hostile actors, including malign states and "domestic disinformers". Once identified, the CIR works with a global network of partners to counter these threats to democracy.

The CIR fulfils its mission through three strands – research and programmes, the Global Investigations Unit and our Resilience Network. We are a collaborative initiative; we work with partners including civil society, the media, grassroots organisations, academia and democratic governments to coordinate activities.

We believe the scale of the problem demands an ambitious, collective response.

