Global Cyber Troops Country Profile: India

By Ualan Campbell-Smith and Samantha Bradshaw
Oxford Internet Institute, University of Oxford

Introduction

On 14 February 2019, a terrorist attack by Pakistan-based terrorist organization Jaish-e-Muhammad in Pulwama district of Kashmir, killed 40 Indian soldiers and triggered a wave of online disinformation. Within 24 hours of the attack, a doctored image of opposition Indian National Congress (INC) party leader Rahul Gandhi standing next to the suicide bomber was debunked by the Indian fact-checking site Boom Live (Poynter, 2019). The Hindi text accompanying the photo questioned whether the INC party was involved – a deliberate attempt at using the attack to incite political tensions (AFP Fact Check, 2019a). Despite best efforts to counter the spread of false and misleading content, disinformation filtered through to credible news outlets, with mainstream channels in India and Pakistan publishing news stories that amplified rumours and misinformation about the attack (AFP Fact Check, 2019b).

The geopolitical incident prompted major concerns, as doctored, misleading and outdated images and videos circulated on social media platforms and reached millions of additional viewers through mainstream media. This could not have come at a more sensitive time: India's 900 million eligible voters – including 340 million Facebook users and 230 million WhatsApp users – will take part in India's general election, the largest exercise of democracy in history.

This short memo provides a brief background on "cyber troop" activity in India. "Cyber troops" are defined as government or political party actors tasked with manipulating public opinion online (Bradshaw & Howard, 2017, 2018). This memo provides an overview of the various tools and techniques used to amplify the spread of "junk news" on social media and suppress the voice and participation of political opponents or vulnerable populations online. Drawing on data from the Global Cyber Troops Annual Inventory,[1] we provide information about the capacity and resources that have been invested into social media manipulation in the lead-up to the 2019 general election.

We found that cyber troop capacity has grown significantly in the lead-up to the 2019 general election. While there were only a few actors involved in social media manipulation in 2017, political parties are now working with a wider-range of actors including private firms, volunteer networks, and social media influencers to shape public opinion over social media. At the same time, more sophisticated and innovative tools are being used to target, tailor, and refine messaging strategies including data analytics, targeted advertisements, and automation on platforms such as WhatsApp. In previous years, we have measured the capacity of cyber troop activity in India as being low. However, the increasing amount of money being spent on growing team sizes, advertising campaigns, and hiring private firms combined with the application of

[1] The Global Cyber Troops Inventory uses a three-pronged methodological approach to identifying instances of social media manipulation by government actors. This involves (1) a content analysis of news article reporting; (2) a secondary literature review; and (3) expert consultations. More information about the approach can be found in Bradshaw and Howard (2017, 2018).

a variety of more sophisticated computational techniques underscores the growing capacity of cyber troops operating in India.

The disinformation following February's terrorist attack in Kashmir served as a warning to social media platforms, citizens, and politicians ahead of the general election. The low barriers to entry, availability of resources, and low levels of regulation on networks such as Facebook, Twitter and WhatsApp provide ample opportunities for propaganda. And an enormous population comprising a variety of castes, religions and languages, with varying levels of digital literacy, provides a fertile ground for disinformation. This, combined with the fact that political parties are deliberately exploiting these vulnerabilities as part of campaign strategies, has meant that disinformation is playing a key role in the 2019 general election.

An Overview of Cyber Troop Activity in India

Organizational Form

India has a long history of political parties using social media for political campaigning. The two main political parties, incumbent Prime Minister Narendra Modi's Bharatiya Janata Party (BJP), and opposition Indian National Congress (INC) party, both have 'IT cells' that are known to use automation, trolling and disinformation techniques. These IT cells have existed since the early days of social media, with the BJP's IT cell founded in 2007.

Political parties in India have also been known to work with private firms. Cambridge Analytica "worked extensively in India" according to whistle-blower Christopher Wylie (CNBC, 2018). The Indian IT firm Silver Touch was responsible for building Modi's NaMo app, and was linked to fake Facebook accounts (Facebook, 2019). Influencers on social media platforms are increasingly used to amplify political messages more organically to a wider audience. For example, Delhi marketing firm OMLogic Consulting has worked for both the BJP and INC to utilize the power of YouTube and Instagram influencers (*The Economic Times*, 2019a).

Although several countries have experienced external interference, cyber troop activity in India is predominantly of domestic origin. The deliberate spread of disinformation by politicians and political parties has often led to misinformation – the accidental spread of false content – as a result of hyper-connectivity and digital illiteracy. However, there have been a few cases of foreign interference by countries such as Pakistan who set up a series of fake accounts and Facebook pages about issues to do with India's general election (Reuters, 2019). Following the Kashmir attack, individuals linked to the Pakistan Army used Facebook and Instagram accounts to inflame tensions with India and push claims over Kashmir (DFRLab, 2019).

Table 1: Organizational Form and Prevalence of Social Media Manipulation in India

Initial Report	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens & Influencers
2007		BJP, INC	Cambridge Analytica, Silver Touch, OMLogic Consulting		Evidence Found

Source: Authors' evaluations based on data collected. Blank spaces indicate no evidence was found.

Strategies, Tools, and Techniques

Cyber troops in India use a variety of strategies, tools and tactics to spread disinformation and manipulate public discussions about politics online. Disinformation often originates from non-credible news outlets or fake social media accounts, but disinformation is prolific in India as it also originates from mainstream media, politicians, and as part of official election strategies. *The Economic Times* and *India Today*, which has its own fact-checking project, published – both in print and in a video – a photo that allegedly showed the February terrorist attacker in a combat uniform; however, in reality it originated from an unknown source on Twitter and was determined as fake (Poynter, 2019). Boom Live claim that political parties have "begun building teams for the specific purpose of pushing out a huge volume of propaganda and disinformation" (The Atlantic, 2018). Both the BJP and INC accuse each other of propagating "fake news" while denying they do so themselves (Reuters, 2018). And Amit Malviya, head of the BJP's IT cell, publicly acknowledged that there was "some scope for misinformation" during the election (Huffington Post, 2019).

Automation is used by political actors in India to create inorganic popularity around an individual, organization, or message. During the 2014 general election, the BJP were accused of paying to artificially boost their popularity on social media. On Twitter, Prime Minister Narendra Modi is second only to United States President Donald Trump as the most followed politician, with 45.9 million followers; however, a study by Twiplomacy (2018) claimed that as many as 60 percent come from fake accounts. There is also evidence of active networks of Twitter bots that are already being deployed ahead of the election to boost Modi's popularity. In February 2019, the hashtag #TNwelcomesModi received 777,000 mentions over two days, in reference to Modi's visit to Tamil Nadu, a southern Indian state. In response, #GoBackModi was mentioned 447,000 times by INC-supporting accounts (Quartz, 2019; DFRLab, 2019). Despite the high levels of automation on Twitter, this activity did not reach very many people, as the unsophisticated fake accounts had few followers.

Trolling tactics have also been used to suppress the political speech and participation of dissenting opinions. In the book *I am a Troll*, Indian journalist Swati Chaturvedi details the creation of the BJP's IT cell, also known as the 'BJP troll army,' which was formed in 2007 by Prodyut Bora to smear and threaten opponents online (Huffington Post, 2018). Today, around 300 workers use "strategies meant to inflame sectarian differences, malign the Muslim minority, and portray Modi as saviour of the Hindus" (Bloomberg, 2018). These attacks vary in their sophistication: from crudely automated criticism, such as #GoBackModi, to highly personalized attacks on individuals. They specifically target political opponents and journalists – especially prominent female figures – with sexual harassment and abuse. Sometimes individuals are also threatened with real-life physical attacks by online trolls (Reuters, 2018). For example, the Office of the United Nations Commissioner for Human Rights called for the government to protect journalist Rana Ayyub, after her face was superimposed on pornographic clips and she received rape and murder threats, following false quotes attributed to her on social media (Guardian, 2018). While parties explicitly deny supporting online trolls, these accounts are often aligned with party agendas and the leaders provide tacit support. For example, Prime Minister Modi follows known troll accounts on Twitter, and drew criticism for hosting 150 social media influencers at his residence in 2015, many of whom who used sexual slurs to harass women online (Guardian, 2018).

Social Media Platforms

In the 2018 Global Cyber Troops Inventory, we found that chat applications were an important platform for spreading disinformation about politics. This is especially true in India: at least 50,000 election-related WhatsApp groups were created by both the BJP and INC during the May 2018 Karnataka state elections (Freedom House, 2018). The social media chief of the BJP declared 2018 the year of India's first 'WhatsApp elections', and has reportedly "drawn up plans to have three WhatsApp groups for each of India's 927,522 polling booths" (Time, 2019). A so-called 'cell phone pramukh' will operate a number of these groups and drive the party's WhatsApp-based campaign by circulating specially designed campaign material (Hindustan Times, 2019). Parties are even using data analytics to form WhatsApp groups based on demographic and socio-economic factors, using information from the electoral roll to sort the population into groups based on factors such as caste and affluence, to achieve micro-targeted messages (Quartz, 2019).

The platform most impacted by disinformation is WhatsApp, and as a result it is increasingly scrutinized by the Indian government. Mob lynchings caused 30 deaths in India throughout 2018, which reportedly resulted directly from misinformation spread over the app – leading them to be known as 'WhatsApp killings' (Guardian, 2019). In one video that went viral in June 2018, footage of a child abduction was accompanied by text about 'kidnappers' arriving in the city to abduct children; however, it was actually a child abduction awareness video created in Pakistan. In line with their trolling tactics, political differences are exacerbated by inciting Hindu–Muslim tensions on WhatsApp. For example, right-wing Hindu groups circulated a video on WhatsApp allegedly depicting a Muslim mob attacking a Hindu woman, but in reality, it was footage of a lynching in Guatemala. Automation has also been attempted; during the state elections in 2018, the platform's systems detected an attempt by someone in Karnataka to create dozens of WhatsApp groups in quick succession (New York Times, 2018). However, the platform has taken several steps to curb crude attempts at automating accounts or forwarding messages. These responses are detailed in the final section on government and platform responses.

In April 2019, Facebook took down 687 pages and accounts linked to the IT cell of the INC which posted about political issues, the upcoming elections, and criticism of the BJP. Facebook also suspended 15 pro-BJP pages, groups and accounts, and one pro-BJP Instagram account linked to Silver Touch. These accounts were not removed because of the content they posted, but because they engaged in "coordinated inauthentic behaviour" (Facebook, 2019).

Alongside evidence of computational propaganda on Twitter, Facebook and WhatsApp, Modi has his own app, NaMo, which launched in June 2015 and has over 10 million downloads. NaMo is a platform used by Modi to communicate with his followers. However, he has received a significant amount of criticism for bypassing traditional media channels and evading media scrutiny through its use (Bansal, 2018). And despite the Indian government putting pressure on social media platforms to control disinformation, there is a lack of content moderation on the NaMo app, making it susceptible to propaganda. One of the most prolific accounts on this app, The India Eye, was responsible for 40 percent of the 744 posts on NaMo's default feed. Alt News – a fact-checking organization in India – uncovered extensive misinformation peddled by The India Eye on their Facebook page: at least six of the 20 most shared posts

between September and November 2018 were inaccurate or misleading, exposing misinformation to its two million followers (Atlantic, 2019). Alt News discovered The India Eye had links with Silver Touch, the private firm linked to fake accounts on Facebook and Instagram. It is also claimed that Silver Touch created the NaMo app itself (The Wire, 2019). The India Eye's Facebook page was taken down by Facebook and is part of a wider propaganda network linked to Silver Touch (Facebook, 2019).

Table 2: Observed Strategies, Tools and Techniques of Social Media Manipulation in India

Fake Accounts	Messaging and Valence	Content	Targeted Ads	Platforms
Human & Automated Accounts	Pro-Party Messages, Attacks on Opposition, Polarization Strategies, Trolling and Harassment	Facebook pages, disinfo/misinfo websites, memes, doctored videos	Facebook Ads	Facebook, Instagram, Twitter, WhatsApp, NaMo

Source: Authors' evaluations based on data collected.

Organizational Capacity and Resources

Networks of paid workers and volunteers disseminate sophisticated disinformation strategies across social media, responding in real time to political developments. The organization of propaganda efforts appears to be both centrally coordinated and volunteer-run. India's vast size and regional politics means that propaganda efforts are geographically coordinated. There is evidence of specific regional cells, such as the Gujarat Congress IT cell's 'Cyber Army' (DFRLab, 2019) and the BJP's 50-member team in an office in Bangalore (Boom Live, 2018). A former troll said that he was given a half-dozen Facebook accounts and eight cell phones as part of a 300-person team in a BJP IT cell (Bloomberg, 2018).

Alongside these paid workers, individuals can volunteer to assist in 'WhatsApp Group Management', being 'active on Facebook & Twitter' or 'Content Creation' among others, according to a volunteer sign-up form (Boom Live, 2018). There is a blurring of attribution between paid IT cell workers and volunteer movements. The former head of the BJP IT cell, Arvind Gupta, said in 2016 that neither the party nor IT cell had ever encouraged trolling, and that online support came from a grass-roots movement (Bloomberg, 2018). Relying on volunteers and paid workers allows the blurring of boundaries between campaigning, trolling and propaganda.

Both political parties used Facebook to target political advertisements at voters. Following the takedown of fake accounts in April, according to Facebook the INC-linked accounts spent US$39,000, and the BJP-linked accounts spent US$70,000 from 2014 to 2019 in political advertisements (Facebook, 2019). However, since February 21, when Facebook began to track political advertising, the total spending for political advertisements in India totalled 103 million rupees, approximately US$1.5 million (New York Times, 2019). There is a lack of transparency on who is amplifying political advertisements; while the top three advertisers in India were all aligned with the BJP's election agenda, none explicitly disclose their affiliation.

Table 3: Cyber Troop Capacity

Team Size	Resources Spent (USD)	Activity Levels	Coordination	Capacity Measure[2]
Multiple teams ranging in size from 50-300 people	$1.5 million on political advertisements. Contracts with several firms for unknown amounts.	Temporary Around Election Periods	Medium levels of coordination between cyber troops. Geographically organized.	Medium

Source: Authors' evaluations based on data collected.

Government and Private Responses

In response to the proliferation of disinformation, there have been a number of public and private initiatives designed to curb the spread of low-quality information online. Fact-checking has been an important response and several media organizations, such as Boom Live and Alt News, have been established to verify photos and rumours spread on social media.

Given its importance to Indian politics and everyday life, WhatsApp has received the most public criticism. Following the rumours spread on WhatsApp, the Indian IT ministry issued several warnings, stating irresponsible messages were not being "addressed adequately by WhatsApp", and that in the absence of adequate checks, WhatsApp would be considered an "abettor" of rumour propagation and subject to legal consequences (Bloomberg, 2018). In response, WhatsApp added a 'forwarded' tag to messages, limited to five the number of times a message can be forwarded, and launched an advertisement campaign giving "easy tips" to spot fake news (Guardian, 2018). Restrictions have proved ineffective, and technical tools to circumvent these restrictions are advertised to campaigners – such as one charging a fee of 0.04 rupees ($0.0005) per message per individual, to allow a message to be forwarded thousands of times (Vice, 2019).

The day following the Kashmir terrorist attack, India's Central Reserve Police Force set up a team of 12 soldiers to fact-check social media posts (LA Times, 2019). Army Chief General Bipin Rawat said that "Our adversary will utilise social media for psychological warfare. We must also leverage social media to our advantage" (Economic Times, 2018). Given the heightened tensions with Pakistan following the Kashmir attack, the Indian army is now considering how to use social media to its strategic advantage. The defence ministry recently approved a new Information Warfare branch of the Indian army in March 2019 (Economic Times, 2019).

Battling disinformation is particularly difficult in India: dozens of languages make both automated and human moderation difficult, and the end-to-end encrypted nature of WhatsApp restricts the platform's ability to counter disinformation. Alt News even found that two of Facebook's media partners, India Today Group and Jagran Media Network, published false information about the Kashmir attack (New York Times, 2019). This demonstrates the difficulty in countering disinformation, and that they are against ingrained and institutionalized practices.

[2] The capacity measure considers team size, levels of coordination, amount of money spent, activity levels, tools and techniques used, and the number of organizational forms. This measure is used to comparatively assess different countries' capacity in the Global Cyber Troops Inventory.

Conclusion

Computational propaganda efforts in India have gained increased prominence and media attention as a result of the 2019 general election. There has been a mounting body of evidence demonstrating the growing capacity of cyber troops in India to carry out social media manipulation campaigns In the lead-up to the 2019 general election, teams have been growing, new techniques have been tried and tested, and private companies have been hired, all to give political parties a cutting edge during the campaigning periods. Given heightened geopolitical tensions, several years of social media manipulation, and institutionalized disinformation practices, these efforts are not set to disappear once the election results are announced. There is a growing recognition of the (geo)political power of social media, which could have an impact beyond the 2019 election as military investments in information warfare come to fruition over the coming years.

References

AFP Fact Check, 2019. https://factcheck.afp.com/no-not-photo-indian-politician-rahul-gandhi-perpetrator-deadly-suicide-attack-kashmir

AFP Fact Check, 2019. https://factcheck.afp.com/no-these-videos-do-not-show-indian-pakistani-warplanes-kashmir

Alt News, 2018. https://www.altnews.in/alt-news-expose-fake-news-peddling-fb-page-the-india-eye-and-its-gujarat-connnection/

Atlantic, 2019. https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/

Bansal, 2018. https://bansalsamarth.substack.com/p/disfact-18-how-fake-news-thrives

Bloomberg, 2018 https://www.bloombergquint.com/law-and-policy/mob-lynchings-whatsapp-at-risk-of-being-labelled-abettor#gs.e25s77kU

Bloomberg, 2018. https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/

Bradshaw, Samantha and Philip N. Howard, 2017. Troops, Trolls and Troublemakers: A Global Inventory of Social Media Manipulation. COMPROP Working Paper Series. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

Bradshaw, Samantha and Philip N. Howard, 2018. Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. COMPROP Working Paper Series. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Boom Live, 2018. https://www.boomlive.in/with-23000-whatsapp-groups-bjps-final-push-to-woo-voters-in-karnataka/

Buzzfeed, 2019. https://www.buzzfeednews.com/article/pranavdixit/india-and-pakistan-were-on-the-brink-of-war-but-a-full

CNBC, 2018. https://www.cnbc.com/2018/07/11/cambridge-analytica-must-answer-india-says-minister-prasad.html

DFRLab, 2019. https://medium.com/dfrlab/electionwatch-inauthentic-activity-in-india-8940588e09b5

DFRLab, 2019. https://medium.com/dfrlab/pakistan-armys-covert-social-network-23ce90feb0d0

Economic Times, 2018 https://economictimes.indiatimes.com/news/defence/soldiers-should-get-access-to-social-media-within-line-of-control-army-chief/articleshow/65668575.cms

Economic Times, 2019. https://economictimes.indiatimes.com/news/politics-and-nation/ahead-of-general-elections-parties-tap-social-media-influencers/articleshow/68208863.cms

Economic Times, 2019. https://economictimes.indiatimes.com/news/defence/defence-ministry-approves-information-warfare-branch-for-indian-army/articleshow/68329797.cms

Facebook, 2019. https://newsroom.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/

Freedom House, 2018. https://freedomhouse.org/report/freedom-net/2018/india

Guardian, 2018. https://www.theguardian.com/technology/2018/nov/12/whatsapp-struggling-control-fake-news-india-bbc-study-hindu-nationalism-cheap-mobile-data

Guardian, 2018. https://www.theguardian.com/world/2018/jun/26/indian-foreign-minister-sushma-swaraj-trolls-social-media

Guardian, 2019. https://www.theguardian.com/technology/2019/feb/06/whatsapp-deleting-two-million-accounts-per-month-to-stop-fake-news

Hindustan Times, 2019. https://www.hindustantimes.com/india-news/bjp-plans-a-whatsapp-campaign-for-2019-lok-sabha-election/story-lHQBYbxwXHaChc7Akk6hcI.html

Huffington Post, 2018. https://www.huffingtonpost.in/2018/06/22/its-like-frankensteins-monster-the-father-of-the-bjps-it-cell-says-team-modi-started-the-rot_a_23464587/

Huffington Post, 2019. https://www.huffingtonpost.in/entry/narendra-modi-app-has-a-fake-news-problem_in_5c4d5c86e4b0287e5b8b6d52?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=hReEnJ5TA7Q1z_OkA4dycg

Los Angeles Times, 2019. https://www.latimes.com/world/la-fg-india-pakistan-fake-news-20190315-story.html

New York Times, 2018. https://www.nytimes.com/2018/05/14/technology/whatsapp-india-elections.html

New York Times, 2019. https://www.nytimes.com/2019/04/01/technology/india-elections-facebook.html

Poynter, 2018. https://www.poynter.org/fact-checking/2018/inside-whatsapps-battle-against-misinformation-in-india/

Poynter, 2019. https://www.poynter.org/fact-checking/2019/no-image-can-be-taken-on-face-value-fake-images-flood-social-media-after-a-terrorist-attack-in-india/

Quartz, 2019. https://qz.com/india/1553765/bjps-whatsapp-ops-is-what-cambridge-analytica-can-only-dream-of/?utm_source=facebook&utm_medium=qz-organic

Quartz, 2019. https://qz.com/india/1590085/bots-boost-gobackmodi-tnwelcomesmodi-ahead-of-indian-election/

Reuters, 2018. https://www.reuters.com/article/us-india-politics-media-analysis/indian-journalists-say-they-intimidated-ostracized-if-they-criticize-modi-and-the-bjp-idUSKBN1HX1F4

Reuters, 2019. https://in.reuters.com/article/india-election-socialmedia-idINKCN1OJ0DR

Reuters, 2019. https://www.reuters.com/article/facebook-accounts-india/facebook-deletes-accounts-linked-to-indias-congress-party-pakistan-military-idUSKCN1RD1R2

The Wire, 2019 https://thewire.in/media/the-indian-eye-fake-news-factory-namo-app-silver-touch

Time, 2019. http://time.com/5512032/whatsapp-india-election-2019/

Twiplomacy,2018. https://twitter.com/Twiplomacy/status/966226775683534848?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E966226775683534848&ref_url=http%3A%2F%2Fwww.newindianexpress.com%2Fnation%2F2018%2Fmar%2F14%2F60-per-cent-of-pm-narendra-modis-twitter-followers-are-fake-twiplomacy-1786939.html

Vice, 2019. https://news.vice.com/en_us/article/597mwk/modis-trolls-are-ready-to-wreak-havoc-on-indias-marathon-election