FEATURE

Assessing India's Preparedness

External Interference in Political Processes through Social Media

Aditya Bharadwaj

Abstract

The Internet has enabled the greatest information exchange known to mankind and has emerged as a great tool. However, with the revelations of Russian interference in the US presidential elections in 2016, questions have arisen regarding how social media could be used to interfere with the political processes of democracies across the globe. Democracy in itself is a fragile system, because it allows the divide within societies to show up front and center. Yet, this is also what makes democracy a durable system of governance. This article seeks to explore the threats posed by interference through social media in the Indian context. While the problems of Indian democracy and systems are not exactly the same as those facing Western democracies and systems, the threats that democratic systems across the world face are very similar, as external forces try to exploit existing divides within societies to achieve their goals. This is compounded by the fact that China, an authoritarian dictatorship, has emerged as a technological power with great amount of the world's data being administered by Chinese companies in opaque ways. Through this article, the author also studies the existing tools that India possesses, legislative and otherwise, to combat these threats and enumerates possible solutions that could perhaps assist in dealing with these threats.

Ipsa scientia potestas est.

(Knowledge itself is power.)

— Sir Francis Bacon

Introduction

The term *information warfare* has been in vogue in the strategic affairs community for a long time. It is a concept that has existed since time immemorial; however, it has evolved to mean different things today. From wartime propaganda to the spread of fake news during critical situations, information warfare has

served as a questionable yet efficacious tactic in governments' arsenals. A robust definition that the US Joint Chiefs of Staff's *DOD Dictionary of Military and Associated Terms* defines *information operations*, those actions taken to conduct information warfare, as, "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[1]

Information systems have undergone a radical change with the introduction and widespread adoption of the Internet and social media. The Internet has made it possible for an open exchange of tremendous amounts of information that would have been impossible a century ago. The Internet's decentralization is what makes it radically different from any other prevalent information system or medium of communication. Its decentralization is what has allowed this openness to proliferate on the Internet and has contributed to the rise of social media. Nevertheless, this has also ensured that the possibility of manipulation and interference has increased manifold. Cyberwarfare, which is a type of information warfare, has thus become a major risk across the globe.

India and the Internet

Indians are getting onto the Internet at a rate faster than ever. Access to cheap data, falling handset prices, and lighter versions of mainstream applications have led to a revolution in Internet access. In the third quarter of 2019, there were 451 million active monthly Internet users, according to a report by the Internet and Mobile Association of India.[2] This number is expected to increase significantly by 2022.[3] It has been nothing short of a revolution.

Indians on Social Media

Though most Indians use WhatsApp, Instagram, Twitter, Facebook, and so forth, there are a new bunch of social media applications mostly owned and promoted by Chinese tech giants that have taken much of the developing world by storm. TikTok, ShareChat, Likee Video, Hypstar, and Injoy are feature prominently among these. For convenience these social media will be collectively referred to as new social media (NSM) hereafter. Most of these apps have perfected the formula to generate a great amount of traction while cultivating a loyal and ever-increasing base. These applications are focused on providing viral content that is mostly video-centric. This is in contrast to social media applications like Facebook, Twitter, or Instagram, which focus more on user-generated content to

be consumed by followers. For convenience, these older social media applications will be collectively hereinafter referred to as traditional social media (TSM).

The NSM's focus on shareable content—content that can be easily exported and shared on other intermediaries like WhatsApp or Facebook—has proved to be a great asset in user base expansion. Another feature that adds to the "*viral-ity*" of content is the use of artificial intelligence (AI)-based algorithms to show content to users in applications like TikTok. This allows TikTok to show a user content even when an individual has no account on the platform or follows and other users, which is radically different from TSM platforms and makes NSM content more viral.[4] TikTok initially uses your location to show content, then, as a user uses it longer, the app analyses the content you are watching by taking into account the faces, voices, music, or objects in videos you watch the longest. Interacting with the content by "liking," "sharing," or "commenting" further helps TikTok figure out a user's preferences.[5]

Misinformation on Social Media

However, this *"viral-ity"* is also where a problem arises. Content on these platforms goes viral extremely quickly. Thus, rumors and fake news go spread rapidly too. Coordinated misinformation campaigns and hate speech are amplified as a result of these AI-based algorithms that are almost always very good at their job.[6] By the time a piece of information can be verified, millions of people have already seen and reacted to it.

A recent example of this can be seen in the coordinated misinformation campaign targeting Indian Muslims. India has a history of Hindu–Muslim conflict, and the current government led by the Bharatiya Janata Party (BJP) is seen as favoring Hindus over Muslims. As the COVID-19 pandemic gripped the world, multiple videos on Tiktok emerged claiming that COVID-19 was nothing but Allah's way of testing a Muslim's devotion. In one of the videos, which is a 17-second clip, Hindi captioning suggests that COVID-19 would not strike Muslims and invokes the Qu'ran in claiming that handshaking and hugging cure disease. These videos were created to prevent Indian Muslims from taking COVID-19 precautions, capitalizing on their distrust of the Indian government. A cybersecurity firm has alleged that most of these videos were of foreign origin with Hindi captioning and Urdu voice-overs.[7] The Indian Ministry of Electronics and Information Technology had asked major social media companies to take action on such videos and keep sharing "daily reports" on measures taken regarding this issue.[8]

Social Media and Political Mobilization

Political Communication through Social Media

There exists a larger trend of political mobilization via social media that has contributed to large-scale protests, movements, and shifts in political trends. A survey taken during the Tahrir Square protests, which took place during the Arab Spring in Egypt, shows how social media has radically changed the methods of political mobilization and communication. Almost half the people surveyed had used Facebook to communicate about the protests.[9] The Arab Spring, a series of protests against ruling regimes in the Middle East from 2010 to 2012, was largely possible because of social media. It allowed activists and protestors to mobilize and issue calls for protests by communicating efficiently and circumventing state-controlled or censored media.[10]

Social media has also played an increasingly prominent role in elections worldwide and has had a great impact on people and their voting patterns. Barack Obama, the US president from 2008 to 2016, has been referred to as the "social media president" for his social media savvy.[11] His campaign was also one of the first to effectively utilize Internet tools, such as e-mail blasts, to effectively campaign and raise great amounts during both his campaigns from small donors.[12] Elections today, have become both offline and online affairs. An Internet presence for parties and candidates has become increasingly important in countries with a social media presence. Rallying support through social media has come to the forefront.

Indian Politics on Social Media

In India, the 2014 general elections for the Lok Sabha were referred to as the nation's first social media election, especially influencing young voters.[13] Another report has indicated that social media had a great impact in influencing the choices of first-time voters in the 2019 general election for the Lok Sabha.[14] Yet, a report by a New Delhi-based think tank Lokniti-CSDS indicates that the effect of social media on determining outcomes of Indian elections has been pretty limited. According to the same report, 33 percent of voters owned a smartphone in 2019, and among voters with a smartphone there is a high proportion of those who use social media. It was also noted that only one in four respondents expressed personal political views online, while over half said they never do it.[15]

Nevertheless, what is stark from the report is the rapid rise of social media between 2014 and 2019. It was noted that Facebook usage increased by three times, WhatsApp usage went up four times, and Twitter usage grew by sixfold in this

period.[16] Even if these figures are taken with a grain of salt and compared with other reports,[17] they show that there has been a great rise in smartphone penetration and Internet penetration, and it is safe to infer that this rise is going to continue in the near future. This view is further cemented by the fact that India's overall Internet penetration stood at 36 percent in 2019,[18] which is comparably low compared to countries like the United States and China, which stood at 90 percent[19] and 61.2 percent[20] respectively, indicating that the Indian market has substantial room for growth.

Unethical Campaigning through Social Media

"Free" Social Media

Political consultants and analysts have identified social media as an effective campaign tool to achieve political ends in recent times. In this process, social media "farms," which promote inorganic spread of political content in a targeted manner for maximum effect during campaigns, have become popular means to influence public opinion during campaigns. While the targeted aspect of advertisements on social media are not necessarily unethical on their own, since targeted advertisements (political or nonpolitical) are how social media companies make money, this is the basic contract template of any "free" social media service. In exchange for the free services that allow users to socialize on their platform, the social media companies collect data on users to show them advertisements. The data collected is processed using proprietary algorithms to ensure users interact with advertisements on these platforms. To protect the privacy of users, the data is supposed to be anonymized so that it cannot lead back to individual users.

Cambridge Analytica Scandal

However, the dangers of a targeted system of advertisements used in political campaigns that was too efficient came to light when the Cambridge Analytica scandal was exposed. Cambridge Analytica was a British analytics firm that helped political campaigns reach voters online. It did so by analyzing data collected on voters from different online sources. When the scandal emerged, the main issue was the unethical ways in which data was collected and privacy of individuals was breached.[21] There was a personality test on Facebook that harvested user data from nearly 87 million users that was sold illegally to Cambridge Analytica to build psychographic profiles of users to enable microtargeting of voters.[22]

What this means is that data was harvested to better understand the personalities of potential voters and build a psychological profile to target voters in a

more precise manner. Despite that, there is nearly no evidence that microtargeting has worked, and there is also potential for such targeting to backfire.[23] Cambridge Analytica's parent company, Strategic Communication Laboratories (SCL), a political consultancy firm, has a history of indulging in corrupt practices in different countries.

The effects of its corrupt actions were especially pronounced in political campaigns in small Caribbean countries. For example, in 2013 SCL, along with the Canadian company Aggregate IQ, set up the first data microtargeting program for the ruling party of Trinidad and Tobago. A former employee of the disgraced Cambridge Analytica notes that this was done under the garb of getting a contract from the ruling party for analysis on certain sectors like health, which serves as a cover for under-the-table political work. In Trinidad, this was done through a contract to build a national police database, using a system that would capture citizens' browsing, record phone conversations, and apply natural language processing to in essence predict which citizens were predisposed to commit crime.[24] Incidentally, SCL claimed in a brochure that it helped a client in Trinidad during the 2010 elections by creating political graffiti in such a way that it "ostensibly came from the youth" and its client could "claim credit for listening to a 'united youth'."[25]

Later, Cambridge Analytica's CEO, Alexander Nix, had claimed that the company had "5000 data points on 230 Million American voters," which is stark considering the fact that USA had 250 Million voters in 2016.[26] This is extremely alarming when it is noted that Cambridge Analytica was involved in high-profile political campaigns that succeeded, such as Donald Trump's 2016 presidential campaign[27] and the Brexit "Vote Leave" campaign.[28]

As noted above, there might not be enough evidence to show that these campaigns based on psychographic profiling are actually successful. Despite that, what is concerning is the way data can be harvested and individual profiles can be made and can be successfully utilized to even attempt to influence political choices of individuals in a tailor-made manner. As technology evolves, the prospect of these tailor-made online political campaign tools getting increasingly accurate is scary and represents a real threat to democracy.

External Interference through Social Media

The Cambridge Analytica scandal and the actions of SCL brought the attention of the world to how players, who were largely internal political actors, could use social media to game the political system using advanced technology. Yet, when external players—for example, other countries—use social media for such activities, it becomes a bigger and more dangerous problem: equivalent to information

warfare. The internal players attempting to use these techniques would still seemingly have a certain level of accountability. However, external players could rarely ever be held accountable for actions of election interference through social media.

It may seem like a distant reality, but, election interference through social media by external forces is here, front and center. The 2016 US presidential election was when this issue came to the forefront. On 6 January 2017, merely days after the inauguration of Pres. Donald Trump, the US Office of Director of National Intelligence released a declassified version of a report titled "Assessing Russian Activities and Intentions in Recent US Elections."[29] This report was a declassified version of an assessment that had been given to the president and the recipients approved by him. It basically outlined how the Russian government made an effort in the 2016 US presidential elections to undermine American democracy. According to the Federal Bureau of Investigation, this was Russia's boldest attempt to influence US elections to date.[30] In the context of this article, we shall specifically focus on the Russian government's use of social media to undermine trust in American democracy and attempt to influence the elections.

Russian Social Media Measures to Interfere in the US Elections

The Russian government sought to undermine Hillary Clinton and promote Donald Trump in the elections and used many strategies to that end. This included hacking operations, strategic leaks, using state-funded overt propaganda and operations on social media.[31]

To elaborate on Russian interference using social media, reliance will be placed on the above cited report by the Office of Director of National Intelligence[32] and the redacted version of the "Report on the Investigation into Russian Interference in the 2016 Presidential Election" by Special Counsel Robert Mueller (hereinafter referred to as the "Mueller Report"). Russia's interference in the 2016 US presidential elections came through a St. Petersburg–based organization called the Internet Research Agency (IRA) funded by a Russian businessman with close ties to Vladimir Putin, the Russian president.[33]

Taking Advantage of the Divide

The IRA started operations targeting the United States as early as 2014 to sow discord in the American political system. The IRA did this by creating multiple fake personas pretending to be US-based activists and later even fictitious US--based organizations on social media. Many of the fake accounts even pretended to be the personal accounts of many Americans, and the IRA ran many "groups" on these platforms. The IRA employees assigned to operate the social media accounts

were called "specialists." These groups and accounts were used to address divisive US political and social issues and became a means to reach large US audiences. By the spring of 2014, the IRA began to consolidate its US operations within a single department called the "Translator" department, which was further subdivided into different teams addressing "operations on social media platforms to analytics to graphics and IT." The IRA's US operations were part of a greater plan called "Project Lakhta."[34]

In July 2014, IRA employees even traveled to the United States on intelligence-gathering missions, collecting information and photographs for later use in their social media posts during these missions. By February 2016, internal documents showed that the IRA efforts were to focus on support of Donald Trump's campaign and opposition to Hillary Clinton's campaign. The IRA, which controlled multiple Facebook groups, even played a great role on-ground campaigns through Facebook. According to Facebook, the organization purchased over 3,500 advertisements, and its expenditures on the platform were around $100,000. IRA--controlled accounts made over 80,000 posts before their deactivation, and these posts reached at least 29 million Americans and "may have reached" an estimated 126 million people, according to Facebook.[35]

In January 2018, Twitter publicly identified 3,814 Twitter accounts associated with the IRA. According to Twitter, in the 10 weeks before the 2016 US presidential election, these accounts posted approximately 175,993 tweets. Twitter also announced that it had notified approximately 1.4 million people it believed may have been in contact with an IRA-controlled account. The IRA also used its social media accounts to hire Americans to carry out on-ground tasks for them such as organizing rallies, taking pictures with political messages, and so forth.[36] The Russian government also aggressively promoted its state-owned news channel Russia Today (later called RT) on social media. RT had substantially expanded its programming, specifically highlighting criticism of alleged US shortcomings in democracy and civil liberties. These actions specifically fell within the aims of the Russian government to undermine the American public's confidence in their government. The Russian establishment had even prepared a Twitter campaign, titled #DemocracyRIP, on election night in anticipation of Hillary Clinton's victory, according to the Office of Director of National Intelligence.[37]

A Real Threat to Democracy

The systematic way in which the Russian government interfered in US presidential elections using social media is extremely noteworthy and qualifies as cyberwarfare. By exploiting the existing rifts in American society and gaming the system, the Russians effectively interfered with the system in an attempt to achieve

Moscow's foreign policy goals.[38] Even if the effects of Russian interference through social media in the US elections were negligible, the actions amplified the divide in American society and dented the American people's trust in the democratic process. And as Abraham Lincoln once noted, "A house divided against itself, cannot stand."[39]

What the above noted events also reflect are the Obama administration and the US national security community's inability to plan for and deal with these threats. With the emergence of the Internet as an effective political tool, such contingencies should have been planned for considering the activities of firms like Cambridge Analytica's in the United States' neighborhood.[40]

This should be a warning sign for countries across the world regarding the kind of threats that are posed by social media becoming a big part of political activities. As commerce, trade, and almost every other industry has gone online, nations around the globe are building cyberwarfare capabilities to protect themselves from attacks.[41]

Preempting Future Threats

India is rising as a global power, and though Internet penetration in the nation is low, it is projected to rise at a great pace. More and more Indians are getting on social media. Though social media in India might still not have become that much of an effective campaign tool yet, it definitely has become a haven for election--related fake news. Facebook had a massive purge of pages that engaged in coordinated inauthentic behavior before the election.[42] Many other social media and instant messaging platforms have tried to prevent the spread of fake news through various campaigns and new initiatives.[43] Though the effectiveness of these measures in curbing the spread of fake news has been quite questionable.

There will come a time in the future when a greater proportion of India's public will be on the Internet and the impact of social media on the Indian politics will be much greater. As we approach such a time, it is necessary that we are prepared to deal with the threats that Indian democracy might face because of it.

Chinese Influence in Social Media

Currently, most social media applications that are used by Indians are either of American or Chinese origin, with Chinese applications taking over rapidly.[44] In the case of the Russian interference, as noted above, the applications were mostly of American origin—Facebook, Twitter and Instagram, and so forth. These companies have taken steps to prevent such actions from taking place on their platform again.[45] The applications being of American origin still gave the US government a

semblance of accountability over these companies. Nonetheless, things are changing rapidly, and fears still persist that Russia could interfere again in the 2020 US presidential elections—with the addition of China and Iran attempting to influence elections too.[46] However, Chinese companies rapidly gaining users in India represent real threats that are more dangerous.

Chinese Control of User Data and Associated risks

China and the Internet

Government control of Chinese software companies is extremely strict. To operate a website in China, a company needs to have an Internet content provider (ICP) license. It is almost impossible to operate an online service without an ICP license, and doing so is fraught with risks.[47] Every social media application operating in China has to have an ICP license. These licenses are quickly and easily revoked if providers do not toe the government line and subsequent applications could be blocked. Beijing exerts great control over content posted on the Internet in China.[48] Furthermore, it has been reported that companies have to facilitate government censorship and surveillance. A popular Chinese messaging app, WeChat, has started using AI for censorship and surveillance. This has led to consequences for ordinary people, and the censorship has also affected people outside China in countries like Canada and Australia with large immigrant Chinese populations.[49] China has consistently been investing in and has made a commitment to becoming the world leader in AI.[50] This is technology that will take the world by storm and has already seen use in quite a few social media companies in China. This can also be seen as Chinese companies have become global leaders in AI-based censorship of content and have even started marketing these services.[51]

Chinese Control of Technology Companies

These technology companies are different when compared to other Chinese conglomerates or big corporations, because state control and access to CCP officials is what allows many nontechnology corporations to become successful. In 2015, 12 of the largest companies in China were state-owned energy corporations and banks.[52] However, when we take a look at the same Fortune 500 list from 2019, the top two positions in China are occupied by Tencent and Alibaba.[53] Both of these corporations are largely private technology companies that have become dominant in the Chinese market because of their offerings. Toward the end of 2019, Alibaba even became the most valuable Asian company.[54] Due to fears regarding the rise of these new technology companies gaining immense access and

power in Chinese society, the government has sought to rein in these companies. Many companies subsequently have been under government scrutiny for preventing spread of "harmful" content.[55] As they have more to lose, these companies have sought to have greater ties to the Chinese Communist Party (CCP) to protect themselves. They have also started to flaunt their connections to the CCP. However, to not alienate foreign investors and governments, these companies have quietly instituted CCP committees within their organizations to "ensure they do not stray away from party objectives."[56] Quite a few tech moguls—most notably, Ma Huateng, also known as Pony Ma, the chairman of Tencent (owner of WeChat and one of China's biggest tech companies) and China's richest man—have also become members of the National People's Congress, which is the rubber-stamp parliament of China.[57] Thus, the boundaries between private companies and the government is being muddied.

The Chinese government, other than exercising control over these tech companies through policy and rules, has also started to exert financial control. State--owned firms have started investing major amounts in tech companies. For instance, when Xiaomi, a Beijing-based smartphone maker, had its initial public offering on the Hong Kong Stock Exchange in 2018, six of the seven anchor investors were Chinese state-owned corporations.[58]

Chinese Information Warfare Strategy

As early as the 1990s, the Chinese government developed a particular strategy to improve upon information warfare capabilities owing to its weaknesses in conventional warfare when compared to the United States or other countries.[59] Analysts had predicted that China could attack vulnerable critical infrastructures in the United States or manipulate domestic public perceptions and, in turn, weaken America's political will to intervene or fight.[60] These attacks do not necessarily have to be in the form of stealing data or hacking. They could be attacks on democracy like the Russian interference in the 2016 US presidential elections. China formed the Strategic Support Force (SSF) whose Network Systems Department is responsible for cyberwarfare in 2015.[61] This force is still transitional and is expected to undergo many changes.[62] It is projected to become an efficient information warfare tool for the Chinese government and an efficient "information umbrella" for the Chinese military system.[63] Concerns around the SSF's capabilities have raised eyebrows around the world, as the SSF, which comes under the Central Military Commission, will definitely not operate like security agencies in democratic countries and will be used to compel private companies to do their bidding to achieve their objectives.[64] Additionally, China passed laws in 2014 and

2017, the National Intelligence Law in particular, that experts say will force Chinese companies to hand in network data whether they want to or not.[65]

Global Concerns around Chinese Control of Data

Global Concerns Regarding Privacy

Globally, concerns are rising about data collection and privacy policies of Chinese social media and technology companies. A class action lawsuit has been filed against TikTok in a US federal court for allegedly sending data to Chinese servers illegally.[66] A report by a think tank closely connected to the Australian government has alleged that China is harvesting data at a massive global scale.[67] Australian members of parliament have also expressed concern over applications like TikTok. going to the extent of calling it "expeditionary or offshore surveillance."[68] American lawmakers too expressed similar concerns about TikTok in a letter to the Director of National Intelligence. The US Army has banned the use of TikTok on all government devices; the Australian Defence Forces have also followed a similar policy.[69]

Chinese companies have processed the data of millions of Indians, and concerns are being raised at all levels. Recently, Indian MPs Shashi Tharoor, Pinaki Misra, and Jayadev Galla raised concerns about applications like TikTok and Helo (another application owned by TikTok's parent company Bytedance).[70] The implications of Russian interference in American elections through social media was immense. However, the potential of Chinese interference through its control of data of Indians and opaque structures around technology companies is much more significant. As a result of the recent China–India border conflict, the Indian government decided to ban TikTok and 58 other Chinese applications, which were deemed "prejudicial to sovereignty and integrity of India, defence of India, security of state and public order" on 29 of June 2020. In the press release of the ban, the ministry noted that it has received many complaints and various reports claiming misuse of some apps for "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India." What is more notable is the next line, which states, "The compilation of these data, its mining and profiling by elements hostile to national security and defence of India, which ultimately impinges upon the sovereignty and integrity of India, is a matter of very deep and immediate concern which requires emergency measures."[71] The release specifically mentions data mining and profiling activities that are the backbone of social media interference.

Threat of Chinese Interference

The effect of Chinese operations against democracies around the world could be much more clandestine, accurate, and hence, potentially even more damaging. The Russian IRA did have access to substantial amount of data through Facebook. However, the amount of data China's SSF or arms of the Chinese state could gain access to is many times greater than what the Russian IRA possessed and would be gained with much more ease. In addition to this, Chinese prowess in AI, which has given them expertise in censorship and surveillance, is a potential game changer. These are concerns that should be treated with great seriousness considering how close Chinese technology companies and the Chinese state are.

Democracies across the world are raising concerns over these matters. Though it is not yet apparent that efforts are being made by China to influence elections through social media, that day could not be far away, considering that China is already trying to interfere in the democratic processes of countries like Australia and New Zealand. New Zealand especially has been facing great risks to its democracy because of Chinese interference.[72] This even led to campaign finance laws in New Zealand being changed, owing to concerns around Chinese interference.[73] There are also increasing concerns in Australia around Chinese political interference. Many reports alleged that China tried to get an "agent" elected to the Australian parliament, with the Australian domestic spy agency even starting an investigation into these claims.[74] This clearly shows that the will to interfere in the political process of democracies exists in the Chinese state.

It is only a matter of time before China tries to weaponize its control over global data. New Zealand, with its small population that is largely insular, is seen as an ideal petri dish for technology companies to experiment with new ideas and tools on their platforms before releasing them to the wider world.[75] It is highly likely, considering these factors, that New Zealand could be a target for social media interference.

China has usually seen India as a secondary threat compared to the United States and Japan. However, the 2017 Doklam stand-off between Indian and Chinese troops changed that belief in Chinese strategic circles. China today sees India as a greater threat, and there is much more talk of "containing India" in these circles since Doklam.[76] As the India–China border standoff of 2020 at Ladakh was under way, leading to the death of 20 Indian soldiers,[77] Australia experienced a massive cyberattack. Australian government sources have blamed China for the attack on government institutions and infrastructure.[78] The risk that India's democracy faces might currently be lower compared to countries like New Zealand or Australia due

to low Internet penetration; however, it is incumbent upon India to be prepared for a future where this form of information warfare is a possibility.[79]

India's Legislative Tools to Deal with Social Media Interference

Cyberwarfare Not Addressed in Legislation

India's legislation dealing with all things online is the Information Technology Act 2000 (IT Act) and the many set of rules made under it. The act is grossly underequipped to deal with present-day threats. The penal provisions in the act, found in Chapter IX and Chapter XI, mainly deal with crimes such as attacks, hacking, and such and are not built to deal with breaches such as election interference through social media.[80] These penal provisions are from a time when cyberwarfare did not figure in Indian policy makers' outlook.

The election interference that takes place through social media cannot be compared to hacking or server attacks or stealing data. It is a murky practice that involves manipulation of existing systems without necessary stealing data or hacking per se. Though these activities may go hand in hand with violation of privacy, they are much more severe in their effects. The only provision that comes close to being applicable in this sense is Section 66F, which deals with cyberterrorism.[81] Even this provision, which was introduced in 2008, does not conceive the possibility of cyberwarfare through social media interference.[82] This is because the language used to define instances of cyberterrorism are the same as some of the other penal provisions, where the "acts" are the same but their consequences are graver.

Data Protection Report

After Justice B.N. Srikrishna, chairmain of the Committee of Experts on Data Protection, submitted the committee's report with many recommendations,[83] the Personal Data Protection Bill was introduced in the Lok Sabha in 2019. It has currently been referred to a standing committee and a report is awaited.[84] The bill omits section 43A of the Information Technology Act, 2000[85] and in turn gives a wider framework for protecting individual privacy.[86] Certain recommendations of the committee have found place in the bill that could partially help in dealing with the abovementioned threats.

The recommendations also propose the creation of a Data Protection Authority (DPA) with many functions, outlined in Clause 41.[87] Some of the proposed responsibilities of the DPA are, "Monitoring and ensuring compliance, with the provisions of the data protection law . . . specifying circumstances where a DPIA

may be required . . . [and] maintaining a database containing names of significant data fiduciaries and their rating in the form of data trust scores indicating compliance with obligations under the data protection law.'[88] The recommendations propose data audits by empaneled auditors under the proposed DPA "whether a significant data fiduciary's processing activities and policies are in compliance with the applicable data protection law."[89] This recommendation has found place in Clause 29 of the bill.[90] Another proposed responsibility of the DPA is advising the Parliament and Central and State governments on measures to be taken to promote protection of personal data. It is also to be tasked with monitoring technological developments and commercial practices that may affect data protection practices.[91]

The bill draws a distinction between *sensitive* and *critical personal data*, offering a higher degree of protection to the latter—going so far as to mandate that both these kinds of data are to be stored in India.[92] While the bill defines what sensitive personal data is, it offers no explanation as to what falls under the categorization of critical personal data.[93] This bill goes on to give a lot of power to individuals to control how their data is processed. It addresses the privacy aspect of the problem of election interference through social media to some extent. However, the bill has not been passed, and it remains to be seen how well the DPA would perform and what its responsibilities would include when it finally becomes law.

Lack of a Cyberwarfare Policy

Even when the Personal Data Protection Bill is passed, India still will not have a comprehensive legislation or stated doctrine to deal with instances of cyberwarfare. Social media interference is only a small part of cyberwarfare and information warfare. While briefly spoken about in the Indian Army's Land warfare doctrine (LWFD) of 2018, the cyberwarfare policy has been criticized as not being as evolved as China's.[94] In the same LWFD, the word *social media* appears only once in the context of public information and perception management under the subheading of "Psychological Warfare." India desperately needs clear doctrine and a dedicated policy directive to deal with both information warfare and cyberwarfare in an effective manner beyond the narrow sense in which the terms are mentioned in the LWFD.[95] Though they are two different planes of warfare, they have increasingly started aligning on social media, as seen from the Russian interference in American elections. Destabilizing nations and their political processes is easier than ever today due to social media. Section 66F of the IT Act is clearly not enough to deal with these threats.[96] Even the National Cyber Security Policy (2013) does not address the aspect of risks arising out of social media interference.[97] Without defining these problems, India will never be able to deal with

them in an effective manner. The definitions in the laws that India adopts must be clear and dynamic, so that as time passes, Delhi will always be ready to deal with these evolving threats.

Indian Cyberwarfare and Defense Capabilities

Currently, India possesses an elaborate structure of surveillance and monitoring, which includes monitoring the Internet. Ten Central Government agencies are officially entitled to monitor and decrypt any information on a computer resource. This list includes the Intelligence Bureau and the Research and Analysis Wing.[98] Nevertheless, no agency that exclusively monitors the Internet has this access under section 69B of the IT Act.[99] At different points in time, different agencies were created to identify threats and monitor the Internet and other communication systems in India. Currently, India has the Central Monitoring System, which allows income tax officials and security agencies to intercept any form of communication over calls or e-mails by sending intercept requests.[100] This system is administered by the Centre for Development of Telematics (C-DOT).[101]

The National Technical Research Organisation (NTRO) is the lead body responsible for technical intelligence in India, which includes cybersecurity, data gathering and processing, and strategic monitoring.[102] The NTRO reports to the National Security Adviser[103] and falls under the National Critical Information Infrastructure Protection Centre, which is deemed as the designated nodal agency (under section 70A of IT Act)[104] to protect all critical information infrastructure, including sectors under five broad headings: (1) power and energy; (2) banking, financial institutions, and insurance; (3) information and communication technology; (4) transportation; and (5) e-governance and strategic public enterprises. Conversely, the Defence Research and Development Organisation is responsible for protecting the information infrastructure of defense and intelligence agencies. While, the Computer Emergency Response Team–India (CERT–IN) will be responsible for protecting all noncritical information infrastructure and collecting all reports on cyberattacks and incidents,[105] it is also supposed to serve as the national agency for incident response under section 70B of the IT Act.[106]

Responding to increasing concerns, the Defence Ministry has approved the creation of an information warfare branch for the Indian Army.[107] Recently, the Indian government approved the formation of the Defence Cyber Agency, consisting of Army, Navy and Air Force personnel under the Integrated Defence Staff tasked with handling cyberwarfare operations.[108]

As is seen above, there are multiple agencies with different mandates. Often, these overlap and create problems, leading to turf wars.[109] This is not good for the country's security situation, and hence, the government needs to take a consolidation exercise and

clearly define roles of organizations and establish protocols for harmonious functioning of these organizations. A cyberwarfare doctrine setting clear priorities is the need of the hour. Further, mandates for the proposed DPA to cooperate with security agencies in identifying privacy breaches will go a long way in identifying patterns of social media interference. Prevention is better than cure, and agencies need to develop techniques to identify these patterns and establish communication mediums with the general public so that the possibility of large-scale external interference in our democracy through social media can be nipped in the bud. None of the agencies mentioned above have been reported to have large-scale capabilities of monitoring social media for such suspicious social media activity.

Conclusion

Democracy is acknowledged as one of the most fragile forms of government, as it depends upon the will of the people for its strength. The will of the people can never be expected to be totally unanimous, and therein lies the beauty of democracy. However, democratic processes are especially vulnerable to external interference. Hence, it is important for democracies across the world—while ensuring that free thought and new ideas prosper—to effectively identify threats and ensure that they do not consume the system.

The Internet has enabled the greatest information exchange in the history of the world, and social media is its catalyst. Measures have to be taken so that disagreement is not allowed to turn into toxic division through misinformation and interference that allow external powers to take advantage of such differences and to advance their own foreign policy goals. India has to be ready to combat these future threats soon considering the fact that China is ahead of the curve and has proven its adversarial nature toward India.

Aditya Bharadwaj

Mr. Bharadwaj is a student of law at Government Law College Mumbai. He is also currently studying Mandarin at the University of Mumbai. His primary interests lie in law & order, securities law, Indian domestic politics, international affairs, and Indian national security policy. He enjoys reading, writing, and traveling in his free time.

Acknowledgment

The author would like to thank Cheshta Tater and Ketayun Mistry for their invaluable comments, as well as Air University Press reviewers and editors.

Notes

1. US Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms,* June 2020, 104, https://www.jcs.mil/.

2. Megha Mandavia, "India has second highest number of Internet users after China: Report," *Economic Times,* 26 September 2019, https://economictimes.indiatimes.com/.

3. IANS, "India to have over 800 million smartphone users by 2022: Cisco study," *Hindustan Times*, 3 December 2018, https://www.hindustantimes.com/.

4. Mallika Rangaiah, "How is Artificial Intelligence (AI) Making TikTok Tick?," *Analytics Steps* (blog), 16 January 2020, https://www.analyticssteps.com/.

5. David Ramli and Shelly Banjo, "The Kids Use TikTok Now Because Data-Mined Videos Are So Much Fun,"*Bloomberg Businessweek,* 18 April 2019, https://www.bloomberg.com/.

6. Nilesh Christopher, "TikTok is fuelling India's deadly hate speech epidemic," *Wired UK*, 12 August 2019, https://www.wired.co.uk/.

7. Ankit Kumar, "Surge in TikTok videos aimed at misleading Indian Muslims over coronavirus precautions," *India Today*, 3 April 2020, https://www.indiatoday.in/.

8. Shreyashi Roy, "Govt Steps in As TikTok Sees Surge in Fanatical COVID-19 Fake News," *The Quint*, 9 April 2020, https://www.thequint.com/.

9. Zeynep Tufekci and Christopher Wilson, "Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square," *Journal of Communication* 62, no. 2 (April 2012), 363, https://doi.org/.

10. Fadi Salem and Racha Mourtada, "Civil Movements: The Impact of Facebook and Twitter," *Arab Social Media Report* 1, no. 2 (May 2011), 2, 24, https://www.arabsocialmediareport.com/.

11. Kevin Freking, "Obama makes his mark as first 'social media' president," *Seattle Times*, 6 January 2017, https://www.seattletimes.com/.

12. Dan Eggen, "Obama fundraising powered by small donors, new study shows," *Washington Post,* 8 February 2012, https://www.washingtonpost.com/; and Alexis C. Madrigal, "Hey, I Need to Talk to You About This Brilliant Obama Email Scheme," *The Atlantic,* 29 November 2012, https://www.theatlantic.com/.

13. Idrees Ali, "Social Media Played Big Role in India's Election," *Voice of America,* 6 June 2014, https://www.voanews.com/.

14. PTI, "Social media plays key role in influencing first-time voters: Report," *Economic Times,* 12 May 2019, https://economictimes.indiatimes.com/.

15. Lokniti, "Social Media and Political Behaviour," *Lokniti-CSDS,* (June 2019), 18–20, 63, https://www.lokniti.org/.

16. Lokniti, "Social Media and Political Behaviour," 22.

17. IANS, "India to have over 800 million smartphone users by 2022: Cisco study," *Hindustan Times*, 3 December 2018, https://www.hindustantimes.com/.

ET Bureau, "Smartphone users expected to rise 84% to 859m by 2022: Assocham-PwC study," *Economic Times,* 10 May 2019, https://economictimes.indiatimes.com/.

18. Mallika Rangaiah, "How is Artificial Intelligence (AI) Making TikTok Tick?," *Analytics Steps* (blog), 16 January 2020, https://www.analyticssteps.com/.

19. Pew Research Center, "Internet/Broadband Fact Sheet," Pew Research Center, 12 June 2019, https://www.pewresearch.org/.

20. Xinhua, "China has 854 mln internet users: report," *Xinhua News Agency,* 30 August 2019, http://www.xinhuanet.com/.

21. Ian Sherr, "Facebook, Cambridge Analytica and data mining: What you need to know" *CNET,* 18 April 2018, https://www.cnet.com/.

22. Aja Romano, "The Facebook data breach wasn't a hack. It was a wake-up call," *Vox,* 20 March 2018, https://www.vox.com/.

23. Brian Resnick, "Cambridge Analytica's "psychographic microtargeting": what's bullshit and what's legit," *Vox,* 26 March 2018, https://www.vox.com/.

24. April Glaser, "How Shady Was Cambridge Analytica," *Slate,* 29 March 2018, https://slate.com/; and Carolle Cadwalladr, "The great British Brexit robbery: how our democracy was hijacked," *Guardian,* 7 May 2017, https://www.theguardian.com/.

25. "Cambridge Analytica-linked firm 'boasted of poll interference'," *BBC*, 25 March 2018, https://www.bbc.com/.

26. Sherr, "Facebook, Cambridge Analytica."

27. Andrew Prokop, "Cambridge Analytica shutting down: the firm's many scandals, explained," *Vox,* 2 May 2018, https://www.vox.com/.

28. Mark Scott, "Cambridge Analytica did work for Brexit groups, says ex-staffer," *Politico,* 30 July 2019, https://www.politico.eu/.

29. Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* ICA 2017-01D (Washington DC: Intelligence Community Assessment, 6 January 2017), 1, https://www.dni.gov/.

30. Statement of Bill Priestap, in "Assessing Russian Activities and Intentions in Recent Elections," Statement for the Record before Senate Select Committee on Intelligence. (Washington, DC: Federal Bureau of Investigation, 21 June 2017), https://www.fbi.gov/.

31. Office of the Director of National Intelligence, *Assessing Russian Activities,* 1–5.

32. Office of the Director of National Intelligence, *Assessing Russian Activities,* 1.

33. Special Counsel Robert Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: US Department of Justice, March 2019), 14, 17, https://www.justice.gov/.

34. Mueller, *Report on the Investigation into Russian Interference*, 14–22.

35. Mueller, *Report on the Investigation into Russian Interference*, 14–26.

36. Mueller, *Report on the Investigation into Russian Interference*, 28–32.

37. Office of the Director of National Intelligence, *Assessing Russian Activities,* 2–10.

38. Office of the Director of National Intelligence, *Assessing Russian Activities,* 1.

39. Abraham Lincoln, "House Divided speech" (speech, Springfield, IL, 16 June 1858), Abraham Lincoln Online, http://www.abrahamlincolnonline.org/.

40. Glaser, "How Shady was Cambridge Analytica".

41. Keith Breene, "Who are the cyberwar superpowers?," *World Economic Forum*, 4 May 2016, https://www.weforum.org/.

42. Nishant Sharma, "Facebook Removes 687 'Inauthentic' Pages Linked to Congress, 15 With Pro-BJP Content." *Bloomberg Quint,* 1 April 2019, https://www.bloombergquint.com/; and Press Trust of India, "Facebook removes nearly 700 pages linked to Congress due to 'inauthentic behaviour'," *Economic Times,* 1 April 2019, https://economictimes.indiatimes.com/.

43. Sankalp Phartiyal, Aditya Kalra, "Despite being exposed, fake news thrives on social media ahead of India polls," *Reuters*, 3 April 2019, https://www.reuters.com/.

44. Junjie, "These Chinese Apps are Growing in Popularity in India," *Pandaily,* 4 April 2019, https://pandaily.com/.

45. Paige Leskin, "Russia's disinformation campaign wasn't just on Facebook and Twitter. Here are all the social media platforms Russian trolls weaponized during the 2016 US elections," *Business Insider,* 19 December 2018, https://www.businessinsider.in/.

46. Alyzia Sebenius, "U.S. Sees Russia, China, Iran Trying to Influence 2020 Elections," *Bloomberg*, 25 June 2019, https://www.bloomberg.com/.

47. Pang Xingpu, "China: Obtaining An ICP License In China: A Business Necessity For Any Web-Based Presence?," Mondaq, 4 January 2018, https://www.mondaq.com/.

48. Elizabeth C Economy, "The great firewall of China: Xi Jinping's internet shutdown," *The Guardian,* 29 June 2018, https://www.theguardian.com/.

49. Sarah Cook, "Worried about Huawei? Take a closer look at Tencent," *Japan Times*, 28 March 2019, https://www.japantimes.co.jp/.

50. Sarah O'Meara, "Will China lead the world in AI by 2030?," *Nature,* 21 August 2019, https://www.nature.com/.

51. Shan Li, "Made-in-China Censorship for Sale," *Wall Street Journal,* 6 March 2020, https://www.wsj.com/.

52. Scott Cendrowski, "China's Global 500 companies are bigger than ever—and mostly state-owned," *Fortune,* 22 July 2015, https://fortune.com/.

53. Daniel Strauss, "These are the 14 largest Chinese companies," *Business Insider India*, 24 July 2019, https://markets.businessinsider.com/.

54. Kentaro Iwamoto, "Alibaba becomes most valuable Asian company as market cap tops $500bn," *Nikkei Asian Review,* 26 December 2019, https://asia.nikkei.com/.

55. Louise Lucas, "Beijing's battle to control its homegrown tech groups," *Financial Times,* 21 September 2017, https://www.ft.com/.

56. Emily Feng, "Chinese tech groups display closer ties with Communist party," *Financial Times,* 11 October 2017 https://www.ft.com/ .

57. Shusuke Tabeta, "Internet executives well represented at China's National Congress," *Nikkei Asian Review,* 7 March 2018, https://asia.nikkei.com/.

58. Louise Lucas, "The Chinese Communist party entangles big tech," *Financial Times,* 19 July 2018, https://www.ft.com/.

Cheang Ming, "Shares of Chinese smartphone maker Xiaomi stumble on their debut, slipping as much as 6%," *CNBC,* 8 July 2018, https://www.cnbc.com/.

59. Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* (Strategic Studies Institute, US Army War College, 2001), 27, www.jstor.org/.

60. Yoshihara, *Chinese Information Warfare*, 7.

61. John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, DC: National Defense University Press 2018), 5, 13, https://ndupress.ndu.edu/.

62. Costello and McReynolds, *China's Strategic Support Force*, 17.

63. Costello and McReynolds, *China's Strategic Support Force*, 5, 36.

64. Chris Bing, "How China's cyber command is being built to supersede its U.S. military counterpart," *Cyberscoop,* 22 June 2017, https://www.cyberscoop.com/.

65. Arjun Kharpal, "Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice," *CNBC*, 4 March 2019, https://www.cnbc.com/.

66. BBC, "TikTok sent US user data to China, lawsuit claims," *BBC,* 3 December 2019, https://www.bbc.com/.

67. Sarah Zheng, "China harvesting data on global scale, Australian report warns," *South China Morning Post,* 15 October 2019, https://www.scmp.com/.

68. ABC, "Concerns over Chinese access to personal data gathered through TikTok," *ABC,* 19 February 2020, https://www.abc.net.au/.

69. Charlie Moore, "The dark threat of TikTok: Australian children and soldiers who use the social media app are at risk of being spied on by the Chinese, MP warns," *Daily Mail Australia,* 19 February 2020, https://www.dailymail.co.uk/.

70. Press Trust of India, "Tiktok Illegally collecting data and sending it to China, says Shashi Tharoor," *Firstpost,* 2 July 2019 https://www.firstpost.com/.

Megha Mandavia, "TikTok's spreading fake news, MPs say in house," *Economic Times,* 5 July 2019, https://economictimes.indiatimes.com/.

71. "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order," *Press Information Bureau* (New Delhi, India: Ministry of Electronics and Information Technology, 29 June 2020), https://pib.gov.in/.

72. Matt Nippert & David Fisher, "Revealed: China's network of influence in New Zealand," *New Zealand Herald,* 20 September 2017, https://www.nzherald.co.nz/.

73. Eleanor Ainge Roy, "New Zealand bans foreign political donations amid interference concerns," *The Guardian,* 3 December 2019, https://www.theguardian.com/; and Zane Small, "Spy within Five Eyes describes NZ's political system as 'compromised' by Chinese influence," *Newshub,* 13 January 2020, https://www.newshub.co.nz/.

74. Sonali Paul. "Australia probes 'deeply disturbing' allegations of Chinese political interference," *Reuters,* 25 November 2019, https://www.reuters.com/.

75. Ashlee Vance, "New Zealand: The Internet's Petri Dish," *Bloomberg,* 25 January 2013, https://www.bloomberg.com/.

76. Suhasini Haidar, "LAC face-off | Doklam was a game-changer for Chinese thought on India: JNU professor Hemant Adlakha," *The Hindu,* 4 July 2020, https://www.thehindu.com/.

77. "India-China clash: 20 Indian troops killed in Ladakh fighting," *BBC,* 16 June 2020, https://www.bbc.com/.

78. IANS, "Chinese hackers suspected behind massive cyber attack in Australia," *liveMint,* 19 June 2020, https://www.livemint.com/.

79. Rangaiah, "Making TikTok Tick?"

80. Information Technology Act 2000 (India).

81. Information Technology Act 2000 (India), s 66F.

82. Information Technology (Amendment) Act 2008 (India).

83. ET Bureau, "Justice Srikrishna committee submits report on data protection. Here're its top 10 suggestions," *Economic Times,* 28 July 2018 https://economictimes.indiatimes.com/.

84. PRS Legislative Research, "Bill Track: The Personal Data Protection Bill, 2019," PRS Legislative Research, accessed 15 April 2020, https://www.prsindia.org/.

85. Information Technology Act 2000 (India), s 43A.

86. Lok Sabha (House of the People), The Personal Data Protection Bill, 17th Lok Sabha, Winter Session, 2019.

87. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (Ministry of Electronics & Information Technology, 2018), 151, https://www.prsindia.org/; and Lok Sabha (House of the People), The Personal Data Protection Bill, 17th Lok Sabha, Winter Session, 2019, cl 41.

88. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *Protecting Privacy, Empowering Indians,* 154.

89. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *Protecting Privacy, Empowering Indians,* 162.

90. The Personal Data Protection Lok Sabha Bill, (Winter Session 2019) cl 29.

91. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *Protecting Privacy, Empowering Indians*, 154.

92. Lok Sabha (House of the People), The Personal Data Protection Bill, 17th Lok Sabha, Winter Session, 2019, (Winter Session 2019), cl 33.

93. Ibid., cl 2(36).

94. Kartik Bommakanti, "Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army," *ORF Occasional Paper* no. 203 (July 2019): 19, https://www.orfonline.org/.

95. Indian Army, *Land Warfare Doctrine – 2018* (New Delhi, India: Indian Army, 2018), 10, https://www.indianarmy.nic.in/.

96. Information Technology Act 2000 (India), s 66F.

97. Lt Col Sanjiv Tomar, "National Cyber Security Policy 2013: An Assessment," *IDSA Comment,* 26 August 2013, https://idsa.in/idsacomments/.

98. ET Online, "10 central agencies can now snoop on "any" computer they want," *Economic Times,* 21 December 2018, https://economictimes.indiatimes.com/.

99. Information Technology Act 2000 (India), s 69B.

100. Anurag Kotoky, "India sets up elaborate system to tap phone calls, e-mail," *Reuters*, 20 June 2013, https://in.reuters.com/.

101. PTI, "Forget NSA, India's Centre for Development of Telematics is one of top 3 worst online spies," *India Today,* 21 March 2014, https://www.indiatoday.in/.

102. Bureau, "National tech research body to be housed in Hyderabad," *Hindu Businessline,*09 April 2011, https://www.thehindubusinessline.com/.

103. Bhavna Vij-Arora, "Dad's army versus terror Flop tag on tech trackers," *The Telegraph,* 30 July 2008, https://www.telegraphindia.com/.

104. Information Technology Act 2000 (India), s 70A.

105. Saikat Datta, "The NCIIPC and its evolving framework," *Observer Research Foundation,* 3 November 2016 https://www.orfonline.org/.

106. Information Technology Act 2000 (India), s 70B.

107. Shaurya Karanbir Gurung, "Defence ministry approves information warfare branch for Indian army," *Economic Times,* 9 March 2019, https://economictimes.indiatimes.com/.

108. Rajat Pandit, "Agencies take shape for special operations, space, cyber war," *Times of India,* 15 May 2019, http://timesofindia.indiatimes.com/.

109. Sandeep Unnithan, "Spy versus spy," *India Today,* 7 September 2007, https://www.indiatoday.in/.