VIRALITY OF SUSPICION

Influence Operations and Democracies

SAMIR SARAN

BEDAVYASA MOHANTY

Influence operations have been used by nations for political purposes for centuries. As early as the 5th century BC, the Chinese philosopher and military strategist Sun Tzu had written about sowing division between the sovereign and the subject to subdue the enemy without fighting. The Arthaśāstra, Chanakya's treatise on war, also records the use of misinformation by the master tactician to both demoralise the enemy as well as inspire his own troops through the claims of false victories (Hegde, 2017). During the Cold War era, the USSR conducted highly sophisticated influence operations in four stages: demoralisation, destabilisation, insurgency and normalisation (Bezmenov, 1984). Today, they are a staple of modern-day espionage.

The Internet's proliferation and its preponderant use for communication have made the domain an attractive target for disinformation from both state and non-state actors. It is hardly surprising then that among the various controversies that have plagued the governance of cyberspace over the last few years, none has grabbed the public's consciousness and, consequently, regulatory attention that influences operations has. This can be attributed to the speed and intensity with which disinformation campaigns travel over the Internet, their trans-boundary effects, the ease of conduct, and the successes that these campaigns have claimed in recent years.

Influence operations can be hard to define because of the breadth of activities that qualify within its remit. While the US military lacks a single definition of influence operations, the RAND Corporation (in a study commissioned by the US Army), defines influence operations as 'coordinated, integrated, and synchronized

application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviours, or decisions by foreign target audiences that further...interests and objectives' (Larson, et al., 2009). The European Parliamentary Research Service explains that disinformation 'is deliberately false information, in particular that supplied by a government (agent)', and hybrid threats as 'coordinated and synchronised actions that deliberately target democratic states and institutional vulnerabilities, through political, economic, military, civil, and information-related means' (Betzen, 2018). Irrespective of the domain through which they are executed, influence operations share some common traits: they tend to be coordinated acts, broadly directed towards achieving political aims, and are usually conducted in a covert manner.

In cyberspace, influence operations can take many shapes: from the manipulation of social media, to selective leaking of information, to astroturfing, or any combination of the above. Generally, the objective of these operations is to leverage the reach of Internet networks, the hyper-targeted nature of social media platforms, and the short attention span of the general public to release false information with the expectation that crowd sourcing will cause its rapid transmission over the medium. Influence operations change public perception and understanding by exploiting existing divides by either introducing falsehoods or giving predominance to certain truths over others. For example, in 2018, over 30 individuals were lynched by mobs in India over suspicion that they were child abductors (Mohanti, 2018). The triggers for these acts of violence were doctored videos and images, warning users that child kidnappers and organ harvesters had been spotted in their areas. These, like most other instances of mob violence in India, have predominantly targeted nomadic tribes, or religious and cultural minorities, leveraging the latent fault lines within society (Gupta, 2018).

In other instances, influence operations involve dissemination of information that may not necessarily be fake, but embellished in a manner that does not represent the truth. In 2016, for instance, legitimate e-mails between Hillary Clinton's campaign manager and media organisations were leaked to promote the narrative that the media was attempting to favour a Democratic Party outcome in the

upcoming elections (Prier, 2017). This had the effect of discrediting the mainstream media as an institution, thus adding a political flavour to attempts of fact-checking and debunking fake news.

A recurring feature in influence operations is the delegitimisation of traditional institutions, such as mainstream media and government agencies, which exacerbates divisions and drives consumers of news towards alternate fringe outlets that are more likely to publish unverified, and often partisan, news. Analysis by Buzzfeed, for instance, found that in the run-up to the 2016 US elections, viral fake news outperformed major news outlets (Silverman, 2016). Since influence operations rely on the dissemination of partisan viewpoints, they often make use of platforms that appeal to their audience's patriotic fervour. Consequently, instead of questioning the veracity of the information, these campaigns appeal to an individual's patriotic duty to share this information widely. As a result, the individual coordinating the campaign is seen not as subversive, but as an advocate of national values.

Today, influence operations have witnessed a resurgence because of the added spheres of interference that the Internet provides. First, operations that were earlier extremely expensive and required the deployment of covert intelligence operatives in foreign territories can now be conducted remotely over social media and blogging networks. The Russian deep state's orchestration of political rallies and events in Germany is well documented (Wagstyl, 2017).

The ability to remotely organise subversive political events also leverages the second strength of the Internet—anonymity. Remote operators that coordinate influence operation campaigns often use pseudonymous profiles and social media handles that appear to the target audience as their well-meaning compatriots.

Third, even upon the discovery of criminal activity by such profiles/handles, their identification and prosecution often relies on cross-border cooperation and sharing of data between law enforcement agencies. This is a time-consuming process and, given the ephemeral nature of electronic evidence, often does not yield operational intelligence. Attribution is especially difficult for campaigns that achieve a certain degree of virality on the Internet, where it can become near impossible to trace the origin of the information/campaign.

Fourth, and perhaps the greatest strength of the influence operations on the Internet lies in the fact that achieving virality does not depend on the sophistication of the message or its ability to add new information. In fact, fake news that is provocative and unencumbered by granular detail tends to travel faster over social media (Chadwick, 2018). Network effects on the Internet ensure that this 'virality of suspicion' can be achieved by even a single user with a large enough follower count, lending legitimacy to the piece of fake content.

In essence, 21st-century influence operations leverage existing pathways that have been built by social media and technology companies. Russia, for instance, used Facebook's hyper-targeted advertisements during the US presidential election in 2016 to spread inflammatory messages on race and immigration to further divide an already polarised voter base (Guynn, et al., 2018). In a world dominated by 'surveillance capitalism' (Zuboff, 2019), where vast amounts of behavioural data is processed every second, this should hardly come as a surprise. Once the pathways for collection and processing of this information have been established, it is only a matter of time before an external actor devises a way to use it maliciously.

Surveillance capitalism, however, is the new normal of the information age. Where disconnecting from the global information infrastructure is not an option, societies must build institutions that are resilient against cyber threats. It is unfortunate that this resilience to external interference may be inversely proportional to how open, diverse and democratic societies are. Two of the most prominent influence operations in the past year against electoral processes in the United States and France are testament to this reality (Noack, 2018). Countries where societal demographics are heterogeneous are more likely to have social and economic fissures that a malicious actor can exploit. Countries, such as Russia and China, where societies are largely homogenous, and where the state exercises significant control over the Internet, are, in comparison, less vulnerable to social media manipulation and subversion from external actors. To be clear, this is not to say that closed homogenous societies guarantee stability. Often, conducting influence operations in such societies is relatively more difficult because of strong censorship laws and dominant surveillance regimes. When citizens in these societies

are not guaranteed fundamental freedoms of expression and privacy, there is little that can be accomplished by external manipulation.

Nonetheless, insecurities about foreign interference plague all countries equally. The potential of 'Information Operations' to disrupt domestic political processes—that governments around the world are concerned about today—was first brought to the fore by groups of countries led by Russia and China. Starting from 2009, Russia, China and a group of smaller states have been calling for an international treaty on information security that codifies informational sovereignty and abstinence from using Information and Communications (ICT) Technologies to interfere with the states' domestic processes (Roigas, 2015). In 2011, a Russian-led coalition wrote to the UN General Assembly, seeking the codification of a norm to 'not use information and communications technologies and other information and communications networks to interfere with the internal affairs of other states or with the aim of undermining their political, economic and social stability'.[1] The United States and other liberal democracies have traditionally resisted any formalisation of the norm on non-interference (Morgus, 2016).

Today, the targets of influence operations are democratic structures, and true success in mitigating their effect lies in strengthening these institutions. Far too often, the news of external interference by adversaries elicits a knee-jerk reaction among target states. For example, in response to the cases of lynching caused by rumours spreading over WhatsApp, the Indian government, in late 2018, introduced amendments to intermediary liability laws. Among other things, the amendments impose an obligation on intermediaries (or communication service providers) to introduce traceability into their systems—the ability to identify the original sender of the message. For platforms that are end-to-end encrypted, this is perhaps technologically impossible. Compliance with the law, therefore, would require companies to roll back encryption over their services. Thus, what began as a response to the need for accountability over Internet platforms can result in compromising the integrity of the platforms on which users rely.

Instead, efforts should be focused on creating counter-narrative mechanisms that dispel disinformation. The close coordination between fact-checkers, official channels and the mainstream media can render many sources of

disinformation unviable. Companies are already exploring ways in which the identification and flagging of coordinated fake news campaigns can be done by artificial intelligence (AI). While this is unlikely to be a silver bullet, automating the process can significantly arrest the spread of malicious content. These pieces of content, flagged as unverified or false, can make users second-guess themselves before disseminating it further. These active measures can be combined with strong penalties that can act as a deterrent against wilfully and maliciously sharing content that has a clear link to violence and public harm.

India's upcoming general elections in April 2019 will no doubt be a testing ground for disinformation campaigns. This is likely to be a two-pronged challenge with the likelihood of disinformation generated both externally and internally. Already India's home-grown social media ShareChat and Helo, with a combined 55 million registered users, witness a near constant stream of fake news content on their platforms (Bansal and Poonam, 2018). While India has yet to experience a coordinated and sophisticated influence operation conducted by a foreign adversary, some experts have claimed that this is likely in the upcoming elections (Bhattacharya, 2018).

Once again, if successful, these campaigns will possibly leverage existing pathways for the dissemination of disinformation. Ahead of the upcoming elections, the Bharatiya Janata Party (BJP) has allegedly set up 1,800 WhatsApp groups to increase its social media outreach with constituents.[2] While one of the stated aims of these groups is to quell fake news, it is likelier that centralised groups of politically like-minded individuals will become a source of, not a roadblock to, fake news. If political parties create intrinsic value in the micro-targeting of messages, then it is unrealistic to imagine that the same infrastructure will not be hijacked by an external actor at a later date. A marketplace of data can serve actors outside of Indian borders just as well as it serves actors within.

Today, it is hard to gauge the true impact of influence operations. Contrary to the explosive nature of their dissemination, the effects of such campaigns can be subtle and take years to manifest. Moreover, the intangible harm dealt to political and democratic institutions, such as the mainstream media, may not be apparent until it is too late. For nations like India that are only now beginning to come to terms with the threat of influence operations,

it would be advisable to reassess the fragility of their democratic set-ups. An aspect that is perhaps unique to influence operations is that even when they are unsuccessful in their stated goal, they can plant seeds of doubt about the legitimacy of institutions that form the bulwark of nations. And for India, a rapidly maturing digital economy, this seed may be all that is needed for an irredeemable loss of trust in her institutions.

◆

NOTES

1. United Nations, General Assembly, 66th Session, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations, addressed to the Secretary-General*, 14 September 2011 (last visited on 12 February 2019). https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.
2. *News18*, 'Ahead of 2019 Polls, Amit Shah Joins 1,800 WhatsApp Groups to "Stem Fake News"', 21 July 2018. Available at: https://www.news18.com/news/politics/ahead-of-2019-polls-amit-shah-joins-1800-whatsapp-groups-to-stem-fake-news-1819301.html (last visited on 12 February 2019).

REFERENCES

Bansal, Samarth and Snigdha Poonam. 2018. 'Fake News and Hate Speech Thrive on Regional Language Social Media', *Hindustan Times*, 14 November. Available at https://www.hindustantimes.com/opinion/how-regional-social-media-platforms-spew-fake-news-and-get-away-with-it/story-s8Kc2s4TKfne0ZRlXNuLuM.html (last visited on 12 February 2019).

Betzen, Naja. 2018. 'Foreign Influence Operations in the EU', European Parliamentary Research Service, July. Available at http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf (last visited on 12 February 2019).

Bezmenov, Yuri. 1984. *Love Letter to America*. Los Angeles: W. I. N. Almanac Panorama.

Bhattacharya, Ananya. 2018. 'Oxford Researchers Warn India of a Fake-news Epidemic as Elections Approach', *Quartz India*, 25 July. Available at https://qz.com/india/1335161/indias-fake-news-crisis-to-worsen-ahead-of-election-oxford-study/ (last visited on 12 February 2019).

Chadwick, Paul. 2018. 'Why Fake News on Social Media Travels Faster than the Truth', *The Guardian*, 19 March. Available at https://www.theguardian.com/commentisfree/2018/mar/19/fake-news-social-media-twitter-mit-journalism (last visited on 12 February 2019).

Gupta, Apar. 2018. 'Don't blame it on WhatsApp: On Rumours and Lynch Mobs', *The Hindu*, 10 July. Available at https://www.thehindu.com/opinion/op-ed/dont-blame-it-on-whatsapp/article24373370.ece (last visited on 12 February 2019).

Guynn, Jessica, Elizabeth Weise and Erin Kelly. 2018. 'Thousands of Facebook Ads Bought by Russians to Fool US Voters Released by Congress', *USA Today*, 10 May. Available at https://www.usatoday.com/story/tech/2018/05/10/thousands-russian-bought-facebook-social-media-ads-released-congress/849959001/ (last visited on 12 February 2019).

Hegde, Manushree. 2017. 'Espionage in Kautilya's Arthaśāstra.' *Pragyata,* 10 April. Available at http://www.pragyata.com/mag/espionage-in-kautilyas-arthastra-345 (last visited on 12 February 2019).

Larson, Eric V., Richard Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell Schwartz and Cathryn Quantic Thurston. 2009. 'Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities.' US: Rand Corporation.

Mohanti, Mayank. 2018. 'WhatsApp Messages and the Mad Mob Lynching: A Timeline', *News18*, 2 July. Available at https://www.news18.com/news/india/whatsapp-messages-and-the-mad-mob-lynching-a-timeline-1798135.html (last visited on 12 February 2019).

Morgus, Robert. 2016. 'The Normative Bait and Switch', *New America*, 1 December. Available at https://www.newamerica.org/weekly/edition-144/normative-bait-and-switch/ (last visited on 12 February 2019).

Noack, Rick. 2018. 'Everything we know so far about Russian Election Meddling in Europe', *The Washington Post*, 10 January. Available at https://www.washingtonpost.com/news/worldviews/wp/2018/01/10/everything-we-know-so-far-about-russian-election-meddling-in-europe/?utm_term=.e0ade4e13fa5 (last visited on 12 February 2019).

Prier, Jarred. 2017. 'Commanding the Trend: Social Media as Information Warfare', *Strategic Studies Quarterly*, 11 (4) (Winter): 50–85.

Roigas, Henry. 2015. 'The Ukraine Crisis as Test for Proposed Cyber Norms', in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn: NATOCCD COE Publications. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Roigas_15.pdf (last visited on 12 February 2019).

Silverman, Craig. 2016. 'This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook', *Buzzfeed*, 16 November. Available at https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook (last visited on 12 February 2019).

Wagstyl, Stefan. 2017. 'German Politics: Russia's Next Target?', *Financial Times,* 29 January. Available at https://www.ft.com/content/31a5758c-e3d8-11e6-9645-c9357a75844a (last visited on 12 February 2019).

Zuboff, Shoshana. 2019. 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.' US: Public Affairs.

◆◆