

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the author(s) and RSIS. Please email to Mr Yang Razali Kassim, Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

# Elections Integrity in Fake News Era: Who Protects, and How?

By Shashi Jayakumar

# **Synopsis**

How are disinformation and fake news threats evolving? What are the key pressure points in democratic societies and what can be done to protect against these threats? How should responsibility by apportioned?

# Commentary

AN INTRIGUING, but all too brief section in the Singapore Parliamentary Select Committee report on Deliberate Online Falsehoods deals with how to protect elections in Singapore against potential foreign interference. The Committee notes that it did not receive detailed analysis as to whether Singapore's electoral laws are sufficiently comprehensive and modernised to combat "the sophisticated methods employed by malicious actors today to undermine elections".

The dangers are clear enough. State sponsored disinformation and subversion can undermine the workings of democratic society, weaken the trust between government and people, and erode pluralism. While it might be difficult for an influence campaign to ensure a particular outcome in an election, it is perfectly feasible, as Former Facebook Chief of security Alex Stamos recently observed, for such a campaign to throw any election into chaos.

## Foreign Disinformation in Singapore & Region

The litany of recent (and indeed ongoing) case history is plain to see. Russian activities during the 2016 US presidential elections received extensive coverage in the Singapore Parliamentary Select Committee report.

The temptation might be to take the report as purely an academic exercise simply

because the Russians might seem far away. This would be a mistake. The Select Committee received a confidential briefing by a security agency in Singapore, detailing how Singapore has been the subject of foreign disinformation operations by *various* states.

There are also other examples close to home. Consider the baffling and still-unexplained rise of a twitter automated account ("bot") army throughout Southeast Asia earlier this year. Its appearance may or may not have been be tied to the Malaysian general election, which saw its twittersphere flooded by pro-government and anti-Opposition messages by bots of unknown origin. The threat therefore is real.

# **The Singapore Context**

Singapore's Parliamentary Elections Act contains clauses prohibiting certain classes of people, such as foreigners, from taking part in any election activity. Of course, this is not a silver bullet. Besides direct elections interference by states, there is the issue of guns for hire in the international corporate sector that offer similar social media manipulation toolkits to the highest bidder.

The most notorious was Cambridge Analytica and its parent, Strategic Communications Limited. Entities like these will likely continue to operate partly in the shadows.

If Singapore authorities have reasonable grounds to believe that the methods they employ on clients' behalf might have a deleterious impact on Singapore, or might influence an electoral outcome in Singapore, then it would be logical for the government to attempt to hold these companies, and certain individuals within them, accountable.

This might seem far-fetched at present, but it would be consistent with the approach taken for Singapore's Transboundary Haze Pollution Act, where individuals within companies thought to be responsible for forest fires elsewhere (that in turn have a negative impact on Singapore) can be held accountable.

This could come through enacting new legislation specifically to curb foreign interference of this type, or through amendments to existing legislation.

#### Social Media Companies

There is also a need to work with social media companies, which are showing belated signs of stepping up to the plate. Facebook set up a "war room" specifically to deal with challenges posed by fake news during the recent elections in Brazil and elsewhere. Despite its efforts in Brazil, false news proliferated across Facebook and WhatsApp during the polarising campaign.

Observers and advocacy groups were concerned in particular with an explosion in the number of well-organised propaganda campaigns (including hoaxes and misleading news) on WhatsApp, seemingly orchestrated by supporters of the eventual far-right victor Jair Bolsonaro. There were calls – not heeded by Facebook, which owns

WhatsApp – for WhatsApp to lower its forwarding limit in Brazil from 20 recipients to five (as it has done in India) in order to reduce the impact of these campaigns.

It is worth pondering, firstly, whether laws are needed that can compel WhatsApp (which is part of Facebook) to do what advocates in Brazil failed to do by suasion, especially in the heat of electoral battle. Secondly, and perhaps more importantly, will companies like Facebook be prepared to open up the inner workings of their war rooms to governments in future elections to allow for real time input, verification and investigation? If no, then should legal means be employed?

Real-world cooperation between the social media platforms and governments will be key. Having these two actors operate in a clearinghouse fashion to settle issues as they come up in the heat of election campaigning is preferable to increasing the burden on the judicial system.

Consider for example the proposed French law on information manipulation. The law, recently passed by the Senate, will allow political parties or candidates to complain about widely spread assertions deemed to be false or "implausible" during the run-up to elections. The general premise has come under a great deal of criticism by free speech advocates, as have the specific provisions which detail how a judge must decide within 48 hours whether the allegedly false information could alter the course of an election.

If these are fulfilled, the judge can order a block on publication. The difficulty is that this places a burden on the judicial system: potentially intractable questions of interpretation may occur, and hasty decisions may be made while facts are still emerging.

#### **What Lies Ahead**

Aggressors are continually honing their methods. Those who set up fake accounts aimed at influencing the United States mid-term elections went through far greater pains to hide their identities than we have seen with the Kremlin-lined Internet Research Agency that interfered in the 2016 US presidential election.

Technology (think Artificial Intelligence, and the use of "Deep Fakes", which can synthesise video and audio in a manner indistinguishable from the real thing) will increasingly feature in the arsenal of subversive actors.

Those playing defence are kept for the most part on the back foot. What this means is that any new laws or amendments to existing ones aimed at combatting fake news and disinformation in or out of an election period will have as far as possible to be future-proof, taking into account these evolutions.

New legal provisions focusing solely on containing the present will quickly become anachronisms.

Shashi Jayakumar is Head, Centre of Excellence for National Security (CENS) and Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg