Close

THE CONVERSATION

Academic rigour, journalistic flair

Your voting preference might be subtly influenced by social media exposure in the lead up to an election. Ellen Smith/AAP

We’ve been hacked – so will the data be weaponised to influence election 2019? Here’s what to look for

February 21, 2019 4.54pm AEDT

Author

Michael Jensen

Senior Research Fellow, Institute for Governance and Policy Analysis, University of Canberra

Prime Minister Scott Morrison recently said both the Australian Parliament and its major political parties were hacked by a “sophisticated state actor.”

This raises concerns that a foreign adversary may be intending to weaponise, or strategically release documents, with an eye towards altering the 2019 election outcome.

***Read more:* A state actor has targeted Australian political parties – but that shouldn't surprise us**

While the hacking of party and parliamentary systems is normally a covert activity, influence operations are necessarily noisy and public in order to reach citizens – even if efforts are made to obscure their origins.

If a state actor has designs to weaponise materials recently hacked, we will likely see them seek to inflame religious and ethnic differences, as well as embarrass the major parties in an effort to drive votes to minor parties.

If this comes to pass, there are four things Australians should look for.

1. Strategic interest for a foreign government to intervene

If the major parties have roughly the same policy position in relation to a foreign country, a foreign state would have little incentive to intervene, for example, in favour of Labor against the Coalition.

They may, however, attempt to amplify social divisions between the parties as a way of reducing the ability of Australians to work together after the election.

They may also try to drive down the already low levels of support for democracy and politicians in Australia to further undermine Australian democracy.

Finally, they may also try to drive the vote away from the major parties to minor parties which might be more favourable to their agenda.

This could be achieved by strategically releasing hacked materials which embarrass the major parties or their candidates, moving voters away from those parties and towards minor parties. These stories will likely be distributed first on social media platforms and later amplified by foreign and domestic broadcast media.

It is no secret that Russia and China seek a weakening of the Five Eyes security relationship between Australia, New Zealand, Canada, the United States, and the United Kingdom. If weakened, that would undermine the alliance structure which has helped prevent major wars for the last 70 years.

2. Disproportionate attention by foreign media to a local campaign

In the US, although Tulsi Gabbard’s polling numbers rank her near the bottom of declared and anticipated candidates for the Democratic nomination, she has received significant attention from Russia’s overt or “white” propaganda outlets, Sputnik and RT (formerly Russia Today).

The suspected reason for this attention is that some of her foreign policy positions on the Middle East are consistent with Russian interests in the region.

In Australia, we might find greater attention than normal directed at One Nation or Fraser Anning – as well as the strategic promotion of Green candidates in certain places to push political discussion further right and further left at the same time.

3. Promoted posts on Facebook and other social media platforms

Research into the 2016 US election found widespread violations of election law. The vast majority of promoted ads on Facebook during the election campaign were from groups which failed to file with the Federal Election Commission and some of this unregistered content came from Russia.

Ads placed by Russia's Internet Research Agency, which is under indictment by the Mueller investigation, ended up disproportionately in the newsfeeds of Facebook users in Wisconsin and Pennsylvania – two of the three states that looked like a lock for Clinton until the very end of the campaign.

What makes Facebook and many other social media platforms particularly of concern is the ability to use data to target ads using geographic and interest categories. One can imagine that if a foreign government were armed with voting data hacked from the parties, this process would be all the more effective.

***Read more:* New guidelines for responding to cyber attacks don't go far enough**

Seats in Australia which might be targeted include seats like Swan (considered a marginal seat with competition against the Liberals on both the left and the right) and the seats of conservative politicians on GetUp's "hitlist" – such as Tony Abbott's and Peter Dutton's seats of Warringah and Dickson.

4. Focus on identity manipulation, rather than fake news

The term "fake news" suffers from conceptual ambiguities – it means different things to different people. "Fake news" has been used not just as a form of classification to describe material which "mimics news media content in form but not in organisational process or intent" but also used to describe satire and even as an epithet used to dismiss disagreeable claims of a factual nature.

Studies of propaganda show that information need not be factually false to effectively manipulate target audiences.

The best propaganda uses claims which are factually true, placing them into a different context which can be used to manipulate audiences or by amplifying negative aspects of a group, policy or politician, without placing that information in a wider context.

For example, to amplify concerns about immigrants, one might highlight the immigrant background of someone convicted of a crime, irrespective of the overall propensity for immigrants to commit crimes compared to native born Australians.

This creates what communication scholars call a "representative anecdote" through which people come to understand and think about a topic with which they are otherwise unfamiliar. While immigrants may or may not be more likely to commit crimes than other Australians, the reporting creates that association.

Among the ways foreign influence operations function is through the politicisation of identities. Previous research has found evidence of efforts to heighten ethnic and racial differences through Chinese language WeChat official accounts operating in Australia as well as through Russian trolling efforts which have targeted Australia. This is the same pattern followed by Russia during the 2016 US election.

Liberal democracies are designed to handle conflicts over interests through negotiation and compromise. Identities, however, are less amenable to compromise. These efforts may not be “fake news” but they are effective in undermining the capacity of a democratic nation to mobilise its people in pursuit of common goals.

***Read more:* How digital media blur the border between Australia and China**

The Russian playbook

No country is immune from the risk of foreign influence operations. While historically these operations might have involved the creation of false documents and on the ground operations in target countries, today materials can be sourced, faked, and disseminated from the relative security of the perpetrating country. They may include both authentic and faked documents – making it hard for a campaign to charge that certain documents are faked without affirming the validity of others.

Most importantly, in a digitally connected world, these operations can scale up quickly and reach substantially larger populations than previously possible.

While the Russian interference in the 2016 US election has received considerable attention, Russia is not the only perpetrator and the US is not the only target.

But the Russians created a playbook which other countries can readily draw upon and adapt. The question remains as to who that might be in an Australian context.

Social media Hacking Fake news Cyber attack Hacking #auspol Election 2019 Federal election 2019