Russia was behind an enormous effort to influence politics in the US and the UK, but was Australia targeted too? In this series, Hacking #auspol, we explore how covert foreign influence operates in Australia, and what we can do about it.

The civic experience of interacting with analogue voting interfaces is as Australian as the demo cracy sausage . Voters are confronted with tiny pencils , plus physical security measures that involve huddling in a cardboard booth and origami-scale folding.

The use of paper ballots – and human counting of those ballots – creates one of the most secure electoral systems imaginable.

And the Australian tradition provides another sometimes under-recognised component of electoral security: compulsory voting . This practice secures against the voter suppression tactics used to undermine elections in the United States.

In the digital era, smartphones are so prevalent that it might seem tempting to move to voting online. In 2013 the Australian Electoral Commission (AEC) explored internet voting . But cyber security experts say: if it ain't broke, don't fix it.

Read more: ***Election explainer: why can't Australians vote online?***

US system an example of what not to do

The problems the US has had with electronic voting provide a perfect illustration of what can go wrong.

Every year hackers and cyber security experts from across the globe converge “In Real Life” (IRL) on Las Vegas to attend one of the world’s largest and longest-running annual hacker conventions: DefCon .

Election hacking has recently gained prominence at DefCon. In 2017 the “Voting Machine Hacking Village” area revealed the cyber vulnerabilities of US election equipment, databases and infrastructure . One participant even “ RickRolled ” a machine by replacing the voter profile with Rick Astley playing his song “Never Gonna Give You Up”.

The DefCon Voting Village showcased electoral system vulnerabilities again this year, as You ng DefCon attendees aged 8-16 competed for prize money to hack into replicas of election results websites to manipulate vote tallies. It took an 11-year-old just 10 minutes to hack into one of the systems.

Read more: ***Lessons in trust from America's experience with electronic voting***

Recent announcements from the White House indicate that cyber-vulnerable elections are more than child’s play. Earlier this month the Trump administration outlined approaches to bolster defence against cyber operations targeting elections .

Where Australia stands on e-voting

After the 2016 federal election, the leaders of both major parties raised the possibility of introducing electronic voting at future Australian elections
.

Electronic voting is a broad church. Since 2001, the ACT has operated locally networked computers in some locations, and 283,669 voters have used the iVote system in NSW elections.

As early as 2007, the AEC piloted electronically assisted voting to enable access for visually impaired voters. It also trialled voting across a secure network for Australian Defence Force personnel serving overseas.

At the 2013 federal election, the AEC piloted the use of electronically certified lists (ECLs) . This technology enables voters to be marked more quickly off voting rolls, thus avoiding the queues caused by that nice person with a pencil and ruler who looks quizzically at your driving licence.

Electronic scanning and counting of ballot papers was introduced in the 2016 federal election, but subsequently became subject to an inquiry.

In cybersecurity, we are fond of pointing out that no digital system is ever truly secure. Moving to comprehensive, end-to-end, online voting should never take place. The risks of disruption to online voting are, and will remain, simply too high.

Vulnerabilities beyond e-voting

Of course there are other vulnerabilities in the Australian electoral system – dependencies in any system lead to vulnerabilities. External dependencies management is essential for security in elections. For governments, such dependencies include the use of private contractors.

In January, the Australian National Audit Office found that transport suppliers and contractors delivering a new Senate ballot scanning system could not meet security requirements. The Australian Signals Directorate warned the AEC that IT security problems could not be resolved in time for election day. Shortly thereafter, the Council of Australian Governments ordered “health checks” of electoral systems.

In June, the Joint Standing Committee on Electoral Matters found that the AEC needed to update its IT infrastructure to support its core election and voter roll management systems.

Foreign adversaries have been accused of attempting to compromise electoral roll systems in the 2016 US election. In response to this threat the Australian government has provided grants to political parties to seek compliance against the top four basic cyber security measures .

Disinformation is a bigger threat

Such initiatives are welcome. But it is unlikely that large parties would be the target of a genuinely subversive measure designed to create disruption.

There are a few options for an adversary seeking to “hack” an election. The first is to “go loud” and undermine the public’s belief in the players, the process, or the outcome itself. This might involve stealing information from a major party, for example , and then anonymously leaking it. Or it might mean, rather than attacking voting machines themselves, attacking and changing the data held by the AEC. This would force the agency to publicly admit a concern , which in turn would undermine confidence in the system.

Read more: ***Russian trolls targeted Australian voters on Twitter via #auspol and #MH17***

In Australia, this approach would not ultimately affect the actual result due to the security of our physical system. Such an obvious breach might be a prize for an adversary, but its actual effect on a nation with compulsory voting would be short-lived.

The real risk to any election is the manipulation of social media , and a more successful and secretive campaign to alter the outcome of the Australian election might focus on a minor party.

An adversary could steal the membership database and electoral roll of a party with poor security, locate the social media accounts of those people, and then slowly use social media manipulations to influence an active, vocal group of voters.

Securing the elections of the future

In June, ahead of the July 28 by-elections, the government set up an Electoral Task Force composed of Department of Home Affairs, the Australian Federal Police, Australian Security Intelligence Organisation and Australian Cyber Security Centre, to guard against foreign interference in future elections.

In an era when foreign influence via social media is likely , this task force should be invested with sufficient powers to analyse social media and compel social media companies to take down foreign adversarial accounts in real time.

Such an approach might feasibly be taken through existing frameworks – too much coordination between the government and social networks could be incompatible with a free and open public sphere. But faced by a challenge with few clear solutions, every available option should be considered.

Meanwhile, calls for, and the development of, digital voting solutions are not going away.

Australian start-up Horizon State has used blockchain technology to create verified, secure voting systems . Horizon

State will
deploy the system in Sumatra
, hoping scale up for future Indonesian elections.

Read more: ***Africa leads the way in election technology, but there's a long way to go***

Not everyone is certain that blockchain will provide an ideal solution. Such approaches are good for developing democracies, where human corruption in officialdom is the major security risk to elections. But in a mature democracy like Australia, sometimes the tried and true traditions are the best defence.

During the Australian 2016 federal election , Twitter added a sausage on bread emoji to the hashtag #ausvotes. This is one election "hack" we can be
happy to celebrate
. But hey, just don't use a knife and fork, alright?

Tom Sear does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.

Authors: Tom Sear, PhD Candidate, UNSW Canberra Cyber, Australian Defence Force Academy, UNSW

Read more http://theconversation.com/government-may-need-new-powers-to-ensure-election-security-in-australia-101252