Cyber

Swimming between the flags: Digital dangers to Australian democracy

Joint Standing Committee on Electoral Matters, Parliament of Australia

Inquiry into and report on all aspects of the conduct of the 2016 Federal Election and matters related thereto

Submission on notice

Tom Sear, UNSW Canberra Cyber

Swimming between the flags: Digital dangers to Australian democracy

Tom Sear, UNSW Canberra Cyber

The internet has transformed transformed politics, and social media influences how political discussion takes place.

Right now we are all immersed in a global internet experiment where 'multiple actors continue to engage in and experiment with online, social media-driven influence operations as a means of shaping political discourse.' State-driven information and influence operations are being carried out on a scale never before experienced.

The internet has evolved into a potent tool of national influence. America's Acting Homeland Security Advisor Rob Joyce recently pointed out that nation states have shifted their focus:

> *from using the cyber realm to steal secrets, to using that realm to impose national power.*

How this power is imposed varies. The internet is vast infrastructure of tools that can be used to strategically manipulate activities for specific tactical gain, and each state uses them in different ways. Yet while each nation has its own style of influence, ironically using the internet to manifest that influence means states are increasingly reliant on remaining open to each other in the digital realm to assert their power. It is hard to maintain rigid digital borders and assert influence at the same time. This is becoming known as 'entanglement'.

Competition and collaboration

In this series we have discussed Chinese and Russian influence measures in Australian social media. Both nation states utilise different tactics. Chinese operations are 'human- or relationship-centric while Russians are operation or effect-centric.'

Chinese Community Party (CCP) information influence in Australia is more subtle and long-haul than the Russian approach. It is also very sensitive to geopolitical events in its target selection. Disinformation is often as much as about what is not being said or astro turfing as much as it is cyber aggression and messages.

Russian infiltration of Australian political discourse on social media, on the other hand, focuses upon creating disruption Russia also seeks predominately to destabilise the civic culture of the target population, whereas China focuses upon securing connection to an ethic and national diaspora, wherever they may be geographically.

But there are some similarities and these reflect a growing cooperation between them. The strategic origins of these approaches go back to the birth of the internet. In December 2016 Russian President Vladimir Putin signed off on a new Doctrine of Information Security. The document emphasised "information-psychological" defence against influence operations and "information support for democratic institutions". Observers noted the similarity between the Russian and the CCP law in the PRC.

'Long-term, strategic competition' has re-emerged from the revisionist powers of Russia and China to challenge the hegemony of the United States. Peer competitors have the capacity for global reach and influence in politics and economics.

The new normal

Australia as a middle power which punches above its weight globally, by projecting politically and military into the world, needs to adjust to the new normal. The 20th century and its cycle of war and peace are over. Instead, Australian political society now functions in the context of an emergent global geopolitics of perpetual competition, which falls short of actual war.

There is a profound stability-instability paradox at the heart of secure sovereignty in the age of the internet. As Jon R. Lindsay argues, the internet is an economic institution where nation states must 'cooperate to compete.' Chinese economic and financial entanglement ensure that complete blocking of data is impossible, based upon the shared design of the Internet, where consistent incentives to openness remain. China and the United States are thus engaged in, as he describes, 'chronic and ambiguous intelligence-counter intelligence contests across their networks, even as the internet facilitates productive exchange between them. '

Influence operations of foreign nation states in Australia exist within this larger context, and specific challenges are required to confront them. China and the US are involved in a geostrategic technology competition. AI, quantum computing and biotech will be central to future warfare, just as there is Baidu, Alibaba and Tencent (BAT) vs Google, Apple, Facebook, and Amazon (GAFA) 'Stack on Stack' conflict will take place over access to hemispherical data archives for machine learning.

Whether these 'Stacks' will replace nation states in the future is an open question. When Google negotiates interacts directly with the European Union and some suggest, China tech companies resemble states. However, for the moment at least the Westphalian System prevails.

The United States currently has information dominance, and China is seeking to develop asymmetric capabilities to neutralize the traditional strengths of the United States in technology. What has been termed Cyber-Enabled Economic Warfare is one way that China has sought to narrow the technological gap with the United States.

The age of entanglement

Paradoxically, 'entanglement' defines geopolitics in the Internet era. Authoritarian societies create their own separate ecosystems of social control surveillance and

economics. But to ensure financial and espionage flows a relatively open internet to the world is required.

Most importantly, China has not successfully become technologically independent and is reliant upon US corporations to supply the software, hardware innovation and training to ensure the system functions.

Equally through, a network of private corporations (such as Twitter, Google and Facebook) facilitate a global internet system that requires open civil society to ensure information and commerce flow freely. This creates an information asymmetries that revisionist powers can exploit. The United States and the Five Eyes require information operations to be clear and attributable, whereas the revisionist powers can influence societies in the 'gray zone' operations.

Data flows in one direction

The Chinese Communist Party is well known for maintaining a supposedly secure Chinese internet via what is known in the West as the Great Firewall. This is a system that can block international internet traffic from entering China, according to the whim of the government. Technically, for the majority of the 751 million people online in China many of the Apps we use to produce and share information are not accessible. Google, YouTube, Facebook, Twitter - VPNs (virtual private networks) theoretically - are blocked. Material not deemed appropriate can be removed. Earlier this year, for example, Peppa Pig was banned and the People's Daily referred to her as 'gangster.'

Chinese President Xi Jinping talks about the idea of "internet sovereignty" or wangluo zhuquan (网络主权). By controlling cross border data flow, he seeks to assert domestic authority within territorial borders.

In China, 751 million people use apps created by Chinese technology companies such as Tencent, Alibaba and Baidu. Traffic within this ecosystem is monitored and censored in the most sophisticated and comprehensive surveillance state in the world. The Chinese government deploys numerous tools to track users, such as facial recognition, and it's building still more. For instance, Alibaba and Tencent manage the "sesame credit" scheme, which tracks a person's "economic and political conformity score". Flexible digital censorship blocks phrases and images, while The worlds largest troll army police and AstroTurf social media expression.

Just like the historical great wall IRL its digital counterpart is one of myth, and complex compromise. Professor Greg Austin at the UNSW Canberra Cyber has observed in his new book Cybersecurity in China, that the foundations of its cyber defences, including in the Ministry of Public Security, remain weak. Cyber security is a sociotechnical system and is undermined from both sides of this equation.

Firewall circumvention technologies, for example, exist and even VPN blocking cannot be completely consistent without blocking all other data flows. Netizens exploit Mandarin homophones and emoji to evade internal censors.

In June 2009 even Google was blocked in China. In 2011, Fang Binxing one of the main designers of the Great Firewall expressed concern that Google was still potentially accessible in China, saying:

It's like the relationship between riverbed and water. Water has no nationality, but riverbeds are sovereign territories, we cannot allow polluted water from other nation states to enter our country.

The water metaphor was deliberate. Water flows and maritime domains define sovereign borders. And water flows are a good analogy for data flows.

What can Australia do?

The internet has pitched politics into the fluid dynamics of turbulence.In the new era of algorithmic governance, micro-participation and the abstraction, financialisation and legally cognisable manipulation of personal data, makes democratic digital politics look chaotic.

While other nations grapple with the best mix of containment, control and openness - digital dams, channels and deltas - to manage the influence of the rest of the world on their people, while also harnessing these flows in an effort to influence populations around the globe, what can Australia do to safeguard our political shores?

The robustness of Australian democracy is the best defence. If Internet-enabled information is now a form of environment, then it is the nature of the political discussion online, and how that could be manipulated, that is worth watching.

Asymmetric advantage in protecting Australian democracy is by design a coordinated approach between private and government, defence sectors and security agencies in collaboration with an educated public.

As the rip currents of global internet influence operations grow more prevalent, making 'web surfing' more dangerous, Australia would be wise to mark out a safe place to swim between the flags. Successful protection from influence will need many eyes watching from the beach.

UNSW CANBERRA CYBER

Northcott Drive, Canberra ACT 2600

Tom Sear, UNSW Canberra Cyber

cyber.unsw.adfa.edu.au

CRICOS No. 00098G
294387577