The internet is now an arena for conflict, and we're all caught up in it

Tom Sear

Most people think the internet operates as a kind of global public square. In reality, it's become a divided arena where conflict between nation states plays out.

Nation states run covert operations on the same platforms we use to post cat videos and exchange gossip. And if we're not aware of it, we could be unwittingly used as pawns for the wrong side.

How did we get here? It's complicated, but let's walk through some of the main elements.

The age of entanglement

On the one hand, we have an information landscape dominated by Western culture and huge multi-national internet platforms run by private companies, such as Google and Facebook. On the other, there are authoritarian regimes such as China, Iran, Turkey and Russia exercising tight control over the internet traffic flowing in and out of their countries.

We are seeing more cyber intrusions into nation state networks, such as the recent hack of the Australian parliamentary network. At the same time, information and influence operations conducted by countries such as Russia and China are flowing through social media into our increasingly shared digital societies.

The result is a global ecosystem perpetually close to the threshold of war.

Because nations use the internet both to assert power and to conduct trade, there are incentives for authoritarian powers to keep their internet traffic open. You can't maintain rigid digital borders and assert cyberpower influence at the same time, so nations have to "cooperate to compete".

This is becoming known as "entanglement" – and it affects us all.

Data flows in one direction

Authoritarian societies such as China, Russia and Iran aim to create their own separate digital ecosystems where the government can control internet traffic that flows in and out of the country.

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.

For the majority of the 802 million people online in China, many of the apps we use to produce and share information are not accessible. Google, YouTube, Facebook, Twitter are blocked. Instead, people in China 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. In 2018, for example, Peppa Pig was banned and the People's Daily referred to her as a "gangster" after she became iconic of rebelliousness in Chinese youth culture.

Complete blocking of data is impossible

A key objective of this firewall is to to shield Chinese society and politics from external influence, while enabling internal surveillance of the Chinese population.

But the firewall is not technologically independent of the West – its development has been reliant upon US corporations to supply the software, hardware innovation and training to ensure the system functions. And since the internet is an arena where nations compete for economic advantage, it's not in the interest of either side to destroy cyberspace entirely.

As cyber security expert Greg Austin has observed, the foundations of China's cyber defences remain weak. There are technical ways to get around the firewall, and Chinese internet users exploit Mandarin homophones and emoji to evade internal censors.

Chinese economic and financial entanglement with the West means complete blocking of data is impossible. Consistent incentives to openness remain. China and the United States are therefore engaged in what Canadian scholar of digital media and global affairs Jon R Lindsay describes as:

chronic and ambiguous intelligence-counter intelligence contests across their networks, even as the internet facilitates productive exchange between them.

That is, a tension exists because they are covertly working against each other on exactly the same digital platforms necessary to promote their individual and mutual interests in areas such as trade, manufacturing, communications and regulation.

Since Russia is less dependent upon the information technology services of the United States and is therefore less entangled than China, it is more able to engage in bilateral negotiation and aggression.

Different styles of influence

If the internet has become a contest between nation states, one way of winning is to appear to comply with the letter of the law, while abusing its spirit.

In the West, a network of private corporations, including Twitter, Google and Facebook, facilitate an internet system where information and commerce flow freely. Since the West remains open, while powers such as Russia and China exercise control over internet traffic, this creates an imbalance that can be exploited.

Influence operations conducted by China and Russia in countries such as Australia exist within this larger context. And they are being carried out in the digital arena on a scale never before experienced. In the words of the latest US Intelligence Community Worldwide Threat Assessment:

Our adversaries and strategic competitors […] are now becoming more adept at using social media to alter how we think, behave and decide.

The internet is a vast infrastructure of tools that can be used to strategically manipulate behaviour for specific tactical gain, and each nation has its own style of influence.

I have previously written about attempts by China and Russia to influence Australian politics via social media, showing how each nation state utilises different tactics.

China takes a subtle approach, reflecting a long term strategy. It seeks to connect with the Chinese diaspora in a target country, and shape opinion in a manner favourable to the Chinese Communist Party. This is often as much as about ensuring some things aren't saidas it is about shaping what is.

Russia, on the other hand, has used more obvious tactics to infiltrate and disrupt Australian political discourse on social media, exploiting Islamophobia – and the divide between left and right – to undermine social cohesion. This reflects Russia's primary aim to destabilise the civic culture of the target population.

But there are some similarities between the two approaches, reflecting a growing cooperation between them. As the US Intelligence Community points out:

China and Russia are more aligned than at any point since the mid-1950s.

A strategic alliance between Russia and China

The strategic origins of these shared approaches go back to the early internet itself. The Russian idea of hybrid warfare – also known as the Gerasimov Doctrine – uses information campaigns to undermine a society as part of a wider strategy.

But this concept first originated in the Chinese People's Liberation Army (PLA). In 1999, Chinese PLA colonels penned a strategy titled Unrestricted Warfare, which outlined how to use media, government, pretty much everything, in the target country not as a tool, but as a weapon.

It recommended not just cyber attacks, but also fake news campaigns – and was the basis for information campaigns that became famous during the 2016 US presidential election.

In June 2016, Russia and China signed a joint declaration on the internet, affirming their shared objectives. In December 2016, Russian President Vladimir Putin signed off on a new Doctrine of Information Security, which establishes how Russia will defend its own population against influence operations.

Observers noted the striking similarity between the Russian document and Chinese internet law.

Russia and China also share a view of the global management of the internet, pursued via the United Nations:

[…] more regulations to clarify how international law applies to cyberspace, with the aim of exercising more sovereignty – and state control – over the internet.

The recent "sovereign internet" bill introduced to the Russian Parliament proposes a Domain Name System (DNS) independent of the wider internet infrastructure.

If the internet is now a site of proxy war, such so-called "balkanization" challenges the dominance of the United States.

Nations are competing for influence, leverage and advantage to secure their own interests. Russia and China don't want to risk an all out war, and so competition is pursued at a level just below armed conflict.

Technology, especially the internet, has brought this competition to us all.

We're entering turbulent waters

Despite its best efforts, China's leaders remain concerned that the digital border between it and the rest of the world is too porous.

In June 2009, Google was blocked in China. In 2011, Fang Binxing, one of the main designers of the Great Firewall expressed concern 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. The internet has pitched democratic politics into the fluid dynamics of turbulence, where algorithms shape attention, tiny clicks measure participation, and personal data is valuable and apt to be manipulated.

While other nations grapple with the best mix of containment, control and openness, ensuring Australia's democracy remains robust is the best defence. We need to keep an eye on the nature of the political discussion online, which requires a coordinated approach between the government and private sector, defence and security agencies, and an educated public.

The strategies of information warfare we hear so much about these days were conceived in the 1990s – an era when "surfing the web" seemed as refreshing as a dip at your favourite beach. Our immersion in the subsequent waves of the web seem more threatening, but perhaps we can draw upon our cultural traditions to influence Australian security.

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.