Nations want to be the ruler of the internet – at least within their own borders

November 14 2014, by Eerke Boiten

There’s no physical fences in cyberspace, that doesn’t mean there’s no border controls. Credit: paolo_cuttitta, CC BY

While there is only one world power on the internet, that situation will not last forever. The internet's underpinning technologies were mostly created in the US, the initial networks were based there – and today the US hosts the majority of the most powerful internet companies. Although the international community has fought minor battles on internet sovereignty for years, the de facto power that stems from this

US-centricism has for a long time seemed acceptable. But with the revelations – not even all following from Snowden – about international mass surveillance by the US and its allies, it's inevitable the gloves have had to come off.

In a replay of an imaginary Cold War nightmare scenario, Russia and China appear to have identified a common enemy. The nations are expected to sign a collaborative cyber-security treaty to "oppose the use of IT and the internet to interfere in the internal affairs of independent states".

There has also been discussion in mainland Europe, particularly Germany, about "Schengen-routing", which would keep internet traffic away from the parts of the network where NSA and GCHQ could easily snoop on them. Edward Snowden has claimed that establishing a "European cloud" may not be effective, however.

Generally there are two main reasons for states to want to take control of the internet: they want to defend against outsiders – and to defend against insiders.

The enemy outside

Effectively the US still claims sovereignty over large parts of the internet. This is not just de facto sovereignty based on the residence of large internet companies and most cloud servers within the US. It is not even because the Snowden files have shown us that the NSA hoovers up most internet traffic. In a recent court case it was established that US law enforcement agencies can demand data from US companies even when it is stored abroad (in this case, Microsoft servers based in Ireland).

The discrimination in NSA procedures and US law that treats US and non-US citizens differently (worse) is also irksome.

Nor are US allies, chiefly Britain, innocent in this context. Unexplained spying by GCHQ abroad is well-documented, with the claims of eavesdropping at climate change conferences the most recent. The explicit extension of the Regulation of Investigatory Powers Act 2000 introduced through this summer's "emergency" DRIP Act also plays a role. The Act's clause 4 allows the interception of communications even relating to activity outside the UK by persons and companies based outside the UK.

For countries such as Russia and China, the threat from outside is more acute given that both countries have problems with territorial conflicts. There have been reports of cyber attacks in both directions between Russia and Ukraine. And China has been suspected of carrying out man-in-the-middle attacks in order to spy on citizens using encrypted connections.

All these show that these countries also have a greater need to take control. Russia, for example, has recently been reported to be investing US$500m to establish a cyber warfare division, for offensive and defensive operations.

The enemy within

When governments tighten their hold over the internet within their own country it's normally a slippery slope towards the restriction of civil rights. The so-called "great firewall of China" is to restrict freedom of expression and access to information for the Chinese population – to control those within, not those without. Google played along with this by censoring search results within China until 2010, when they moved their operations to the slightly freer jurisdiction of Hong Kong.

Amnesty International has taken up cases of people persecuted for political use of the internet in countries such as Bahrain, Azerbaijan and

Egypt. North Korea has even gone as far as closing down all access to Twitter and Facebook.

On the other hand, Russia is close enough to Europe to not want to be painted as a politically repressive country. Instead Russia controls its internet through more subtle means. For example, its compulsory identity verification for social networks is justified as a defence against identity theft. While many nations operate a blacklist to restrict access to child pornography sites and those distributing copyrighted material, the Russian government added some independent news sites to the list, allegedly to prevent unauthorised protests – and pages on social network VK were highlighted by public prosecutors as advocating terrorism.

However, with its recent explicit attacks on freedom of speech, it seems Russian authorities no longer feel especially restrained in exercising censorship. Putin's claims to support online freedoms like any other democratic country sound a bit shrill taken alongside his description of the internet as "a CIA project".

Setting an example

Not that the UK emerges as a shining example in this respect. Dubious laws have been used to arrest a peer joining a demonstration – and years of spying on eminent historians by MI5 has just come to light. Meanwhile the police feel free to spy on journalists, prison staff listen in on MPs' phone calls and intelligence agencies breach client-lawyer privilege. So it's hard to swallow claims made by the home secretary, Theresa May, and GCHQ that efforts to improve mobile coverage and use encryption shouldn't be allowed because of "security threats".

Of course with elections around the corner, the major parties are making promises about restoring civil rights and establishing safeguards and oversight. But it seems there's been little progress towards David

Cameron's promises in 2009 to erode the "control state" his government inherited.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation