Review to cast light on high value of NZ intelligence networks

By Andrew Colarik and Rhys Ball

March 25, 2015

http://www.stuff.co.nz/national/politics/opinion/67497312/Review-to-cast-light-on-high-value-of-NZ-intelligence-networks

Livelihoods rely on protecting our nation's IT infrastructure, explain Defence and Security lecturers Andrew Colarik and Rhys Ball.

This year New Zealand expects to see the first five-yearly review of its intelligence community, as promised by the National Government in 2013.

This undertaking was given after a number of legislative amendments, including changes to the Government Communications Security Bureau (GCSB) Act, which were made as a result of some particularly revealing official reports; the most significant of which was to become more commonly known as the Kitteridge Report.

The 2015 review will not only further illuminate our intelligence community, but more importantly, show us the value that these organisations collectively bring to our country.

The purpose of our intelligence community is to support the Government managing risks to New Zealand's national security.

The review is obviously necessary, but also timely and relevant amid ongoing enlightenment of the activities of some of our intelligence agencies thanks to Edward Snowden.

Whatever the veracity to these most recent claims, one thing is clear that like it or not, every single day we rely more and more on cyberspace.

Whether we are checking emails, connecting with friends, or just reviewing the day's events, these activities are even more evident when they become unavailable for even a short time.

Our dependence, or rather our interdependence on cyberspace impacts our daily lives in so many unseen ways.

When you buy that overly-priced cafe latte after purchasing petrol for your car on your way to work, we are benefiting from a massive communications infrastructure that provides transportation logistics on a scale few fully grasp.

If it's not made here, we import it from somewhere else and we use the same communications infrastructure for the distribution of our own goods and services.

The standard of living of a nation rests with its ability to export its goods and services and New Zealand has made a considerable investment towards this end.

According to the New Zealand Sectors Report 2013, the size of the information and communications technology (ICT) sector is approximately $8.4 billion (2010) or approximately 6.2 per cent of GDP for the same year.

This makes the ICT sector bigger than health and community services, government administration and defence, and on a par with the agriculture, fishing and forestry sector.

Let's not forget that this information infrastructure provides the very backbone of the banking and finance sector.

The reality is quite simple. New Zealand has a huge information infrastructure investment that affects us all and needs to be protected.

In 2007, the tiny nation-state of Estonia discovered the hard way that its highly integrated country could effectively be digitally isolated from the rest of the world for nearly a month. Imagine what a month of digital isolation would do to this economy.

This is a very real threat among a host of other active cyber-attacks occurring every day.

While we know that many common threats take the form of scammers, phishers and malicious programmers, both here and abroad, cyber criminals will continue to use cyber space to seek and exploit our personal information, steal business information, data records and ideas. But we also know of the cyber-spies - other nation-states wanting to gain knowledge of protected government information for both financial and political purposes.

So from an individual with a laptop and time on their hands - all the way to a country with the resources only a state can muster the dangers of living in, and relying on, a cyberworld are very real.

But who is responsible for the protection from all of these attacks - real and potential?

Is there an expectation that the Government should lead the way and do we trust those who are given this responsibility? If officials have suggested that "national and economic security of New Zealand depends on the reliable functioning of critical infrastructure" then it is clear that this becomes a national security issue.

We have seen how this has been developed overseas - many countries now have established and regularly updated national cyber-security strategies designed to counter these very real problems.

It makes sense that cyber-security be considered a national security priority, but we wait with much interest to see how those conducting the review prioritise New Zealand's national security issues.

We believe that cyberspace and the national information infrastructures it relies upon should be at the top of the list.

The first New Zealand cyber-security strategy was published four years ago.

New initiatives like the cyber-defence system Project Cortex announced last year, may tell us that the Government is addressing the challenges associated with cyber-security, but will it be enough?

And how can we measure its success when an organisation like the GCSB cannot say how the system will work.

Again, tricky challenges but very important and necessary ones, if we are all to engage and actively participate in reducing security risks that have the potential to impact on all citizens.

- Dr Andrew Colarik is a senior lecturer at Massey University's Centre for Defence and Security Studies, and will be launching Massey's first postgraduate Cyber-Security Course in July.

- Dr Rhys Ball is a lecturer at Massey University's Centre for Defence and Security Studies and teaches intelligence studies.

- The Dominion Post