When cyber-terrorists attack close to home

Archived Print Edition
| Darren Greenwood | Friday July 13, 2012

No longer the stuff of sci-fi fantasy, cyber terrorism is real and cyber terrorists are already wreaking havoc.

And rather than New Zealand's geographical isolation helping it, the country's global location puts it at greater risk, because enemies will find online threats easier to deliver than sending in ships.

Recent events have seen the stake rise in the global battle, with Britain's MI5 director-general Jonathan Evans revealing how cyber attacks by a foreign state saw a British company lose $NZ1.6 billion in revenue.

Mr Evans warned "thousands" of people were behind state-sponsored cyber espionage and organised cybercrime. Global jihadists were also using the "Arab Spring" to foment hostile action.

Last month, Eugene Kaspersky, whose lab discovered the Flame virus that attacked computers in Iran, said only a global effort could stop a new era of "cyber terrorism."

"It's not cyber war, it's cyber terrorism and I'm afraid it's just the beginning of the game … I'm afraid it will be the end of the world as we know it," Kasperksy told reporters in Tel Aviv.

Researchers believe Flame was built for the same nation or nations that commissioned the Stuxnet worm that attacked Iran's nuclear programme in 2010.

Kaspersky won't say who he thinks created Flame but said the US, China, Russia, Britain, Israel, and possibly India, Japan and Romania had the technical ability.

Other major attacks, such as the 2007 cyber attacks against Brazil's power grid and Russians attacking networks in Estonia also in 2007, have also been seen.

Though New Zealand might not be at the front line, local security experts warn the country is still at risk.

Two of them, Dr Andrew Colarik and Associate Professor Lech Janczewski from the University of Auckland's Business School have warned of major cyber attacks this year.

Dr Janczewski said attacks could arise from anyone disgruntled at the government, be it domestically or something New Zealand did on the international stage.

"It [the government] could be punished as an example of who not to do business with, politically, economically or even socially," Dr Colarik said.

“We warned of cyber war and all indications are it is accelerating. Just look at the latest disclosure about the latest digital weapon ‘Flame.’ Escalation is almost always the outcome,” he said.

Dr Hanke Wolfe, a cyber security expert at Otago University highlighted “cyber espionage” as many attacks were done for monetary or commercial gain.

“This is not a minor issue – the whole world runs on IT,” he said.

Thus, New Zealand must be prepared. Dr Janczewski cited the widespread use of mustard gas in World War I but in World War II people on both sides were prepared for a gas attack – so gases were not used. Businesses and governments needed to make the same preparations today to avoid the casualties that would occur from a major cyber terrorist attack.

“All of us are at risk” from cyber attacks, according to the New Zealand government.

As part of its cyber security strategy, it created the National Cyber Security Centre (NCSC) last September, established within the Government Communications Security Bureau, to help protect government and other infrastructure providers.

The NCSC has three main functions: providing advice and support to help develop secure networks; detect and respond to sophisticated cyber threats; and co-ordinate and assist operational responses to major cyber events of national importance.

A 2011 incident summary says it and its predecessor, the Centre for Critical Infrastructure Protection, had reported 90 different cyber-security related events.

Almost half of the events involved phishing, compromised credentials and denial of service attacks. Almost half also originated from overseas.

Some 27% of such attacks were directed at government agencies and 4% were directly targeted at critical national infrastructure providers.

The New Zealand government is working with other governments on various exercises to tackle what they see as a global problem.

“These exercises help identify potential vulnerabilities and help assess the effectiveness of planned responses,” a spokesman for the Department of Prime Minister and Cabinet said.

“The government recognises the threat of cyber intrusions and the global nature of that threat. That is why it has a cyber security strategy and the NCSC to provide a co-ordinated response to increasing cyber security in New Zealand,” he said.

Kiwi firms join the battle

New Zealand businesses Endace and the Wynyard Group are joining governments and corporates in fighting cyber crime and cyber terror.

Wynyard provides risk management software to help organisations manage their threats and create measures to mitigate and detect them.

Endace provides software that can record computer activity so, when an incident happens, organisations can detect exactly when and where an attack happened, so they can contain the problem.

Endace corporate marketing vice-president Tim Nicholls said cyber terrorists differed from traditional terrorists in that terrorists sought headlines but the cyber variety had financial or political aims.

For example, Endace worked with banks to help them assess how many credit card details were stolen or with other corporates looking to see who was trying to steal their intellectual property.

Endace also supplied its software to intelligence agencies who used it for “lawful interception,” he said.

Mr Nicholls said just the threat of an attack was damaging as it forced governments and others to spend time, money and effort preparing a defence.

“There are certain states having a go at everybody. You can say with surety New Zealand will have been attacked but, whether the attacks were successful, no one knows,” he said.

Although Mr Nicholls said the UK was at greater risk thanks to the London Olympics, Wynyard’s Craig Richardson said a cyber attack could originate from within a system, waiting for instructions from outside on what was a global battlefield.

“The real risk with cyber terrorism is the unknown unknowns and that’s why intelligence-led risk management is critical,” he said.

Be paranoid

Organisations need to be paranoid and believe cyber criminals and terrorists are out to get them.

John McDonald heads Symantec’s security response team in Tokyo, where he monitors the internet, analysing the threats, malware and devising programs to combat them.

Sensors used “a variety of means” to filter internet traffic and combat the threats, he said.

New Zealand was as much at risk from cyber terror and cyber crime as other countries because, online, geography did not matter. It was about how connected a country was.

“We are finding threats every day. Trojans, threats targeting specific areas, companies, countries. It’s going on all the time,” he said.

Governments and corporates needed to install the best security practices and systems, rather than relying on simple anti-virus software.

“The bad guys have found a way around, so you need to use the latest systems, which are designed for the latest threats,” he said.