

Action stations as cyber attacks on Australia soar

Sarah Whyte

March 14, 2011

More than 400 cyber attacks have affected Australian government networks in the past year, figures reveal.

From January last year to this January there were 405 cyber incidents, an increase from 220 in the previous year, some of which were "very sophisticated", Department of Defence figures obtained by this website show.

One of the attacks by internet activist group Anonymous, called Operation Titstorm, took down the then prime minister Kevin Rudd's website and the parliamentary website in February last year. The parliamentary website crashed for three days after being bombarded with 7.5 million hits a second.

Attacks such as this should not be seen as "legitimate forms of protest activity but rather are public nuisance akin to vandalism", a spokeswoman for the Attorney-General's Department said.

Figures show cyber attacks on government networks are increasing. Between January 2009 and January last year there were about 220 reported incidents and tip-offs relating to Australian government networks, the Defence Department data revealed. These were reported to the Cyber Security Operations Centre, which has operated for the past two years.

The department said it was not prepared to comment on other "specific instances" of intrusion but warned that Australia was experiencing increasingly sophisticated attempts to infiltrate networks in the public and private sectors.

"The threat of unauthorised intrusions into Australian networks is real, rapidly evolving and will continue to test our defences," a spokesman said.

ASIO had created a unit to combat cyber spying, Attorney-General Robert McClelland told the National Security College dinner last week.

Known as the cyber espionage branch, it has been formed in the past nine months and is believed to be under the control of ASIO's counter-espionage and interference division.

"These attacks can be staged from anywhere in the world," Mr McClelland said. "They can infiltrate the control systems of critical infrastructure, be activated remotely, causing damage and mayhem to our technology-dependent lives."

Graham Ingram, general manager of the Australian computer emergency response team, which has worked with the government against cyber attacks, says the most serious ones came from other countries.