GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Monitoring the internet – what the GCSB does and doesn't do

The GCSB is a 'SIGINT', or signals intelligence agency meaning we specialise in intelligence derived from electronic communications. The GCSB has a statutory role in signals intelligence and information assurance and cybersecurity activities.

Everything the GCSB does needs to be in accordance with the objectives in the Intelligence and Security Act 2017 and in accordance with New Zealand's human rights obligations. All of the GCSB's intelligence activity is guided by the Government's National Security and Intelligence Priorities.

The New Zealand intelligence agencies do not have the legal authority, technical means, resourcing, or indeed the social licence to monitor all of the country's internet activity. For example agencies cannot monitor all traffic to particular web sites and chat rooms or who is up loading certain types of material.

The GCSB is able to intercept the communications of New Zealanders for intelligence gathering purposes if it acquires a Type 1 warrant under the Intelligence and Security Act 2017. In order to obtain such a warrant the activity must be shown to be both necessary and proportionate.

To be able to conduct this sort of monitoring New Zealand would also require an access programme that would enable the bulk collection of internet traffic entering and leaving the country. New Zealand does not have such an access programme. Whilst the initial analysis of internet traffic would be done in an automated way it would also require a significant number of skilled people to do the analysis and reporting. Importantly, due to the massive data volumes involved you would need to start with a substantive lead, or compelling hypothesis.

Increasingly internet traffic is encrypted or involves closed chat rooms, which means activity would not necessarily be easily detected. This is not a problem unique to New Zealand. Law enforcement and security intelligence agencies around the world are dealing with the extreme challenges encryption present. Persons of Interest can also deploy tactics to further obfuscate their activity, such as using code words and purposeful misspellings.