Fake mobile towers in central Oslo may snoop on politicians, report reveals

Published time: December 14, 2014 13:44

Norwegian Parliament in Oslo. (AFP Photo/NTB Scanpix/Terje Bendiksby)

A network of fake base mobile stations that can snoop on leading politicians' mobile phones, as well as ordinary people, has been discovered in central Oslo, some outside Norway's parliament and the prime minister's residence, according to a report.

Investigative journalists from the Aftenposten newspaper have detected a number of places in the capital with suspicious mobile activity. They teamed up with two security companies to help track down fake base stations, which confirmed that spy equipment has been used in downtown Oslo.

According to the newspaper, false base stations, known as IMSI catchers, have been most probably used to monitor the movements of high-ranking officials, specifying who enters parliament, government offices and other buildings in the area. It could also be used to snoop on phone calls of selected people in the area.

An IMSI catcher (International Mobile Subscriber Identity) is a telephony eavesdropping device for monitoring mobile phone traffic and movement of mobile phone users. IMSI catchers are used in a number of countries, including the US, by law enforcement and intelligence agencies.

Under Norwegian law, only the National Security Agency (NSM) and police are authorized

to use eavesdropping equipment.

The Security service (PST) has launched an investigation in central Oslo, following the Aftenposten report, to find out who installed the surveillance equipment.

The Local has quoted security operatives as saying that a number of organizations could be responsible for the false base stations.

"It could be private actors or state actors," the PST's Arne Christian Haugstøyl said.

"I can't on the basis of these discoveries say that it is a foreign intelligence agency, but I can say that we know that foreign intelligence agencies have this kind of capacity. And in our preventive work we advise those looking after Norwegian interests not to talk about sensitive issues on mobile phones," he noted.

Visit the ASP Website: http://www.advancedsecurityprotection.com/services/technical-surveillance-countermeasures-tscm-debugging