


## New Zealand accuses China of hacking parliament, condemns activity

Lucy Craymer :: 3/26/2024



New Zealand's Foreign Minister Winston Peters poses for a picture in Wellington, New Zealand January 31, 2024. REUTERS/Lucy Craymer [Purchase Licensing Rights](#) , [opens new tab](#)

WELLINGTON, March 26 (Reuters) - The New Zealand government said it had raised concerns on Tuesday with the Chinese government about its involvement in a state-sponsored cyber hack on New Zealand's parliament in 2021, which was uncovered by the country's intelligence services.

The revelations that information was accessed through malicious cyber activity targeting New Zealand's parliamentarian entities comes as Britain and the U.S. [accuse China](#) of a widesweeping cyber espionage campaign. Both New Zealand and Australia have condemned the broader activity.

Advertisement · Scroll to continue

"Foreign interference of this nature is unacceptable, and we have urged China to refrain from such activity in future," New Zealand's Foreign Minister Winston Peters said in a statement.

He said concerns about cyber activity attributed to groups sponsored by the Chinese government, targeting democratic institutions in both New Zealand and the United Kingdom had been conveyed to the

Chinese ambassador.

Advertisement · Scroll to continue

A top New Zealand intelligence official told a parliamentary committee on Tuesday that seven of its citizens had provided training to China's military in the last 18 months, in what he said was a "major national security risk".

A spokesperson for the Chinese Embassy in New Zealand said in an email that they reject "outright such groundless and irresponsible accusations" and have expressed their dissatisfaction and resolute opposition with New Zealand authorities.

"We have never, nor will we in the future, interfere in the internal affairs of other countries, including New Zealand. Accusing China of foreign interference is completely barking up the wrong tree," the spokesperson said.

The government said earlier on Tuesday its communications security bureau (GCSB), which oversees cyber security and signals intelligence, had established links between a Chinese state-sponsored actor known as Advanced Persistent Threat 40 (APT40) and malicious cyber activity targeting New Zealand's parliamentary services and parliamentary counsel office in 2021.

Advertisement · Scroll to continue

The GCSB said APT40 is affiliated with the Ministry of State Security.

It added APT40 had gained access to important information that enables the effective operation of New Zealand government but nothing of a sensitive or strategic nature had not been removed. Instead, the GCSB said it believed the group had removed information of a more technical nature that would have allowed more intrusive activity.

In the last financial year, 23% of the 316 malicious cyber events that involved nationally significant organisations were attributed to state-sponsored actors, according to the GCSB.

These attacks were not specifically attributed to China and New Zealand last year also condemned malicious cyber activity undertaken by the Russian government.

"The use of cyber-enabled espionage operations to interfere with democratic institutions and processes anywhere is unacceptable," said Judith Collins, the minister responsible for the GCSB.

U.S. and British officials late on Monday filed charges, imposed sanctions, and accused Beijing of a sweeping cyber espionage campaign that allegedly hit millions of people including lawmakers, academics and journalists, and companies including defence contractors.

American and British officials nicknamed the hacking group responsible Advanced Persistent Threat 31 or "APT31", calling it an arm of China's Ministry of State Security. Officials reeled off a laundry list of targets: White House staffers, U.S. senators, British parliamentarians, and government officials across the world who criticized Beijing. Defence contractors, dissidents and security companies were also hit, officials from the two countries said.

A joint statement from Australia's Foreign Minister Penny Wong and Home Affairs Minister Clare O'Neil said persistent targeting of democratic institutions and processes has implications for democratic and open societies like Australia. It said this behaviour is unacceptable and must stop.

In 2019, Australian intelligence determined [China was responsible](#) for a cyber-attack on its national parliament and three largest political parties before the general election but the Australian government never disclosed officially who was behind the attacks.

Andrew Hampton, Director-General of Security at New Zealand's Security Intelligence Service, told a parliamentary committee on Tuesday that seven citizens had left their roles at companies providing training to China's military.

"The training and expertise they were passing on was gained through previous employment with partner militaries and the New Zealand Defence Force," he said. "Such activity clearly poses a major national security risk."

The Reuters Daily Briefing newsletter provides all the news you need to start your day. Sign up [here](#).

Reporting by Lucy Craymer; Editing by David Gregorio, Lincoln Feast and Michael Perry

Our Standards: [The Thomson Reuters Trust Principles](#). 