

POLITICS

China believed to be behind major cyber attack on Australian governments and businesses

By political reporter [Georgia Hitch](#) and political editor [Andrew Probyn](#)

Posted Fri 19 Jun 2020 at 9:20am, updated Wed 15 Jul 2020 at 2:38pm



PM says Australian organisations are being targeted by a "sophisticated, state-based actor" (Pic: ABC News - Matt Roberts)

Federal Government agencies believe that China is the nation behind ongoing cyber attacks on Australian institutions, including hospitals and state-owned utilities, in recent months.

Prime Minister Scott Morrison said Australian organisations, including governments and businesses, were currently being targeted by a sophisticated foreign "state-based" hacker.

While Mr Morrison said the Government would not take the formal step of publicly naming which state, senior sources confirmed China is believed to be behind the malicious attacks.

The Prime Minister emphasised the attacks "hadn't just started", were ongoing and constant threats to Australia, and said the accumulation of attacks required a firm warning to the government and private sectors to harden their shields.

Some of the attacks have been on state government departments and agencies and local governments, all of which hold sensitive economic and personal data.

"This activity is targeting Australian organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure," Mr Morrison said.

Key points:

- China is believed to be behind the wide-ranging attacks on Australian governments and businesses
- The Prime Minister says there have not been large-scale personal data breaches
- The Government will not say publicly which state is behind the cyber attack

"We know it is a sophisticated state-based cyber actor because of the scale and nature of the targeting and the tradecraft used."

Mr Morrison said, so far, it did not appear there had been any "large-scale" breaches of people's personal information, but described the attacks as "malicious".

"This is why we are raising this matter today," he said.

"To raise awareness of this important issue, to encourage organisations, particularly those in health, critical infrastructure and essential services, to take expert advice and implement technical defences to thwart this malicious cyber activity."

Federal Labor Leader Anthony Albanese said he received a full briefing on the ongoing attacks and the work being done by intelligence agencies.

"There is no difference between the Government and Opposition on these issues, none," he said.

Mr Albanese said there had "clearly been an increase" in the number of attacks, which in turn prompted the Prime Minister to issue the warning to Australian businesses and organisations this morning.

PM declined to point the finger at China

When asked whether the country responsible had been identified, Mr Morrison said the Federal Government would not be making "any public attribution" about the attack.

"What I can confirm is there are not a large number of state-based actors that can engage in this type of activity," Mr Morrison said.

According to the Council on Foreign Relations, China, Russia and Iran [are the top three states suspected of sponsoring cyber operations](#).

The chief executive officer of the Cyber Security Cooperative Research Centre (CSCRC), Rachael Falk, said while people may want to point fingers at particular countries, attributing blame was a "distraction".

"It doesn't matter where it comes from to be honest with you," she said.

"This message, the Prime Minister, was clear ... do what you need to do to protect your valuable business and personal data.

"Threats come from anywhere, every day of the week."

Ms Falk said even simple things like making sure passwords were secure and security updates on mobile phones were done as soon as they are released would help secure personal information.

She said calling out the country responsible should be left to the Government and the Australian Signals Directorate, if and when they chose to.



Rachael Falk says Australians should focus on protecting their own data.

Attacks to be expected but PM urges people to be vigilant

Today's announcement comes after the Prime Minister issued a similar statement [last year following attacks, again from a state-based actor, on the major political parties](#).

The Prime Minister said he raised the issue today "not to raise concerns" but to make sure the public was aware of the threat.

"That fact that these threats present is not a surprise in this world in which we now live," Mr Morrison said.

"The actions that we are taking are the actions that we need to take and we will continue to be as vigilant as we possibly can be."

When asked what the motivation of the hackers was, Mr Morrison said it was difficult to pinpoint exactly what it "might be".

"What is of interest to us is that it is occurring and what we are focused on is the practices that they're employing," he said.

"We have some of the best agencies in the world ... working on this and that means that they are putting all of their efforts into thwarting these attempts.

"I can confirm that they have thwarted many, but this is a very complex area."

Defence Minister Linda Reynolds said the Australian Cyber Security Centre and Department of Home Affairs had published a detailed technical advisory today, which outlined what organisations could do to "detect and mitigate" the threat.

"I remind all Australians that cybersecurity is a shared responsibility of us all," she said.



Prime Minister says Australia is being targeted by state-based cyber actors

Editor's note July 15, 2020: This article's headline was changed on June 19, 2020, to clarify that China was believed to be the state behind this cyber attack.