Australia joins international partners in attribution of malicious cyber activity to China

foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china

Joint media release with:

- The Hon Karen Andrews MP, Minister for Home Affairs
- The Hon Peter Dutton MP, Minister for Defence

19 July 2021

Today, the Australian Government joins international partners in expressing serious concerns about malicious cyber activities by China's Ministry of State Security.

In consultation with our partners, the Australian Government has determined that China's Ministry of State Security exploited vulnerabilities in the Microsoft Exchange software to affect thousands of computers and networks worldwide, including in Australia. These actions have undermined international stability and security by opening the door to a range of other actors, including cybercriminals, who continue to exploit this vulnerability for illicit gain.

The Australian Government is also seriously concerned about reports from our international partners that China's Ministry of State Security is engaging contract hackers who have carried out cyber-enabled intellectual property theft for personal gain and to provide commercial advantage to the Chinese Government.

Australia calls on all countries – including China – to act responsibly in cyberspace. China must adhere to the commitments it has made in the G20, and bilaterally, to refrain from cyber-enabled theft of intellectual property, trade secrets and confidential business information with the intent of obtaining competitive advantage.

Since 2017, Australia has publicly attributed malicious cyber activity to North Korea, Russia, China and Iran. Most recently, Australia joined more than 30 international partners to hold Russia to account for its harmful cyber campaign against SolarWinds. Australia calls out these malicious activities to highlight the significant risk they can pose to Australia's national security or to international stability, which in turn can undermine business confidence and inclusive economic growth.

Australia's cyber security posture is strong, but there is no room for complacency given the online threat environment is constantly evolving. Protecting Australia from malicious cyber activity – be it by state actors or cybercriminals – requires a continuous improvement approach to cyber security practices across all levels of society including government, business and households.

The Australian Government will continue to work with international partners and the private sector to strengthen cyber security, including through the implementation of Australia's *Cyber Security Strategy 2020* and *Australia's International Cyber and Critical Technology Engagement Strategy*. All Australians are encouraged to visit cyber.gov.au for advice on how to protect themselves online.

Media enquiries

- Minister's office: (02) 6277 7500
- DFAT Media Liaison: (02) 6261 1555