Minister for Law Enforcement and Cyber Security

Hon. Angus Taylor MP

Australian Government attribution of the 'NotPetya' cyber incident to Russia

16 February 2018

The Australian Government has joined the governments of the United States and the United Kingdom in condemning Russia's use of the 'NotPetya' malware to attack critical infrastructure and businesses in June 2017.

Based on advice from Australian intelligence agencies, and through consultation with the United States and United Kingdom, the Australian Government has judged that Russian state sponsored actors were responsible for the incident.

Computers were infected by a sophisticated piece of malware – or malicious software – that masqueraded as ransomware.

'NotPetya' interrupted the normal operation of banking, power, airports and metro services in Ukraine. While the brunt of the impact was felt in Ukraine, the malware spread globally, affecting a number of major international businesses causing hundreds of millions of dollars in damage.

The Australian Government condemns Russia's behaviour, which posed grave risks to the global economy, to government operations and services, to business activity and the safety and welfare of individuals.

The Australian Government is further strengthening its international partnerships through an International Cyber Engagement Strategy to deter and respond to the malevolent use of cyberspace.

The Government is committed to ensuring the Australian public sector, businesses and the community are prepared for evolving cyber threats.