Attribution of malicious cyber activity in Georgia by Russian Military Intelligence

Media release
21 February 2020

Today, the Australian Government has joined international partners to condemn malicious cyber activity by Russia targeting the state of Georgia in October last year.

In consultation with our partners and allies, the Australian Government has determined that the GRU, Russia’s military intelligence service, carried out a series of disruptive cyber actions against a range of Georgian web hosting providers that resulted in widespread defacement of several thousand websites in October 2019.

Websites affected included sites belonging to the Georgian government, courts, NGOs, media and businesses. These disruptive operations also interrupted the service of several national broadcasters.

A month before Russia’s malicious cyber activity against Georgia, I co-sponsored with the United States and The Netherlands the Joint Statement on Advancing Responsible State Behaviour in Cyberspace in New York in the margins of UN Leaders Week.

This Statement and Australia’s International Cyber Engagement Strategy recognise Australia’s role in safeguarding the benefits of an open, free and secure cyberspace – now and for future generations – and underscore our commitment to upholding the international rules-based order in cyberspace.

This commitment requires us to hold states accountable when they act contrary to the agreed framework of responsible state behaviour in cyberspace.
The international community – Russia included – has agreed that international law and norms of responsible state behaviour apply in cyberspace. This malicious cyber activity contradicts Russia's attempts to claim it is a responsible actor in cyberspace and demonstrates a continuing pattern of reckless Russian GRU cyber operations against a number of countries.

There must be consequences for malicious behaviour in cyberspace. When it is in our interest to do so, Australia considers a range of measures, including public attribution, to respond to malicious cyber incidents, especially those with the potential to undermine global economic growth, national security and international stability.

We will not stand by when cyberspace is used to destabilise democracies, undermine institutions or disrupt critical infrastructure.

Russia has previously agreed to act in accordance with the framework of responsible state behaviour in cyberspace. Australia calls on Russia to fulfil its commitments under that framework.

Media enquiries

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