UK condemns Russia's GRU over Georgia cyber-attacks

The UK, Georgia and international partners have exposed the GRU's – Russia's military intelligence service – responsibility for a number of significant cyber-attacks against Georgia last year.

The National Cyber Security Centre (NCSC) assesses with the highest level of probability that on 28 October 2019 the GRU carried out large-scale, disruptive cyber-attacks. These were against a range of Georgian web hosting providers and resulted in websites being defaced, including sites belonging to the Georgian Government, courts, NGOs, media and businesses, and also interrupted the service of several national broadcasters.

These cyber-attacks are part of Russia's long-running campaign of hostile and destabilising activity against Georgia. The UK is clear that the GRU conducted these cyber-attacks in an attempt to undermine Georgia's sovereignty, to sow discord and disrupt the lives of ordinary Georgian people. The UK remains unwavering in its support for Georgia's sovereignty and territorial integrity.

The Foreign Secretary Dominic Raab said:

> The GRU's reckless and brazen campaign of cyber-attacks against Georgia, a sovereign and independent nation, is totally unacceptable.
>
> The Russian Government has a clear choice: continue this aggressive pattern of behaviour against other countries, or become a responsible partner which respects international law.
>
> The UK will continue to expose those who conduct reckless cyber-attacks and work with our allies to counter the GRU's menacing behaviour.

The UK's National Cyber Security Centre (NCSC) assess that the GRU was almost certainly (95% +) responsible for defacing websites, cyber-attacks and interruption to TV channels in Georgia in October 2019.

Further details on the framework used by the UK government for all source intelligence assessments, including the probability yardstick, are available here.

Given the NCSC's assessment and the broader context, the UK government has made the judgement that the GRU was responsible.

The cyber programme responsible for these disruptions is known in open source variously as the Sandworm team, BlackEnergy Group, Telebots, and VoodooBear.

It is operated by the GRU's Main Centre of Special Technologies, often referred to by the abbreviation "GTsST" or its field post number 74455.

This is the first significant example of the GRU using cyber-attacks to disrupt or destroy since late 2017. This Unit of the GRU was responsible for:

- BlackEnergy: December 2015 shut off part of Ukraine's electricity grid, with 230,000 people losing power for between 1 – 6 hours.
- Industroyer: December 2016 shut off part of Ukraine's electricity grid, also known as CrashOverride. It resulted in a fifth of Kyiv losing power for an hour. It is the first known malware designed specifically to disrupt electricity grids.
- NotPetya: June 2017 destructive cyber-attack targeting the Ukrainian financial, energy and government sectors and affecting other European and Russian businesses
- BadRabbit: October 2017 ransomware encrypted hard drives and rendered IT inoperable. This caused disruption including to the Kyiv metro, Odessa airport, Russia's central bank and two Russian media outlets

Georgia is a strategic partner to the UK. The UK supports a range of projects in Georgia and our annual Ministerial-level UK-Georgia Strategic Dialogue provides an important framework for continuing to develop our strong relationship. The UK was particularly grateful for Georgia's firm support following the attack on Salisbury in 2018, including in efforts to strengthen the OPCW.

Further information