

# 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**

---

## **[General Lorimer: Time for urgent action for new government](#)**

Lieutenant General Sir John Lorimer, the UK's Defence Senior Adviser to the Middle East and North Africa, ended a one day visit to Lebanon on Tuesday 18 February. General Lorimer held high level meetings with Lebanese officials, accompanied by British Ambassador Chris Rampling and Defence Attaché, Lieutenant Colonel Alex Hilton.

His meetings included discussions with President Michel Aoun, Parliamentary Speaker Nabih Berri, Deputy Prime Minister and Defence Minister Zeina Akar, and Lebanese Army Commander General Joseph Aoun.

General Lorimer discussed the current situation in Lebanon, and the role of the Lebanese Army and Security Forces in maintaining security and stability as the sole legitimate defender of Lebanon.

At the end of his visit, General Lorimer said:

This is a crucial time for Lebanon and its new government as it tackles huge economic challenges. Urgent action is needed. I held constructive meetings with Lebanese officials and reaffirmed UK's support to the Lebanese Armed Forces who are key to Lebanon's security, stability and sovereignty. Our partnership and friendship between our armed forces continues.

Ambassador Chris Rampling said:

There should now be no delay on the detailed economic plan the government has promised, the necessary decisions, and urgent implementation. Time is running out. This crisis needs an inclusive and urgent response to the legitimate demands, with calm and clear judgement on what lies ahead.

---

## **DAO 01/20 The Orange Book**

[unable to retrieve full-text content]'Dear Accounting Officer' letters provide advice on accountability, regularity, propriety, value for money and annual accounting exercises.

---

## **The VMD's old GSI email address will no longer work from 1 April**



The VMD moved to its new email address [@vmd.gov.uk](mailto:@vmd.gov.uk) in August 2019.

From 1 April emails sent to our old address [@vmd.defra.gsi.gov.uk](mailto:@vmd.defra.gsi.gov.uk) will no longer be re-directed to our current address.

If you are not using our new address please start doing so as soon as possible and update your records and circulation lists accordingly.

Published 20 February 2020

---

## [Birmingham pharmacist jailed for trafficking Class C drugs](#)

In January, Sarfraz Hussain, 49, of Birmingham pleaded guilty to four counts of supplying Class C controlled drugs and three counts of possession of Class C drugs with intent to supply.

He admitted to supply or intending to supply a total of 1,443,036 doses of controlled drugs with a street value calculated at between £854,000 and £1.4 million.

Hussain, who operated three pharmacies out of Small Heath, Erdington and Halsowen, never held a Home Office Controlled Drugs licence that allows someone to trade, import or export controlled drugs. Despite this, Hussain still ordered large amounts of Class C drugs from legitimate suppliers, prompting the MHRA to inspect his Erdington pharmacy.

When initially questioned about the orders, Hussain denied any wrongdoing, before further investigations revealed that from August 2015 to September 2016 he unlawfully supplied 31,537 packs of Class C drugs, including Zopiclone, Diazepam, Nitrazepam, Zolpidem and Zopiclone.

MHRA enforcement officers seized 560,000 Diazepam, Nitrazepam and Zopiclone tablets from Hussain's three pharmacies.

Mark Jackson, MHRA Head of Enforcement said:

"It is a serious criminal offence to sell controlled drugs which are also prescription only medicines without a prescription.

"We work relentlessly with regulatory and law enforcement colleagues to identify and prosecute those involved.

"Those who sell medicines illegally are exploiting vulnerable people and have no regard for their health. Prescription-only medicines are potent and should only be taken under medical supervision."