UK exposes attempted Russian cyber interference in politics and democratic processes

By Foreign, Commonwealth & Development Office

Published: 2023-12-07 · Archived: 2026-04-05 16:46:40 UTC

- the KGB's successor agency, the Federal Security Service (FSB) is behind sustained unsuccessful attempts to interfere in UK political processes
- targets include politicians, civil servants, journalists, NGOs and other civil society organisations
- in response, the Foreign, Commonwealth and Development Office has sanctioned individuals involved in the group's activity and summoned the Russian Ambassador

The UK and allies have today (December 7th) exposed a series of attempts by the Russian Intelligence Services to target high-profile individuals and entities through cyber operations. The UK Government judges that this was done with the intent to use information obtained to interfere in UK politics and democratic processes.

Centre 18, a unit within Russia's Intelligence Services, the FSB, has been identified as being accountable for a range of cyber espionage operations targeting the UK.

The activity was in turn conducted by Star Blizzard; a group that the UK's National Cyber Security Centre (NCSC) – a part of GCHQ – assesses is almost certainly subordinate to FSB Centre 18.

While some attacks resulted in documents being leaked, attempts to interfere with UK politics and democracy have not been successful.

Star Blizzard is also commonly known as Callisto Group, SEABORGIUM or COLDRIVER and is operated by FSB officers. The group has also selectively leaked and amplified the release of information in line with Russian confrontation goals, including to undermine trust in politics in the UK and likeminded states.

In particular, the UK has identified the FSB - through the activity conducted by Star Blizzard - as being involved in the following:

- targeting, including spear-phishing, of parliamentarians from multiple political parties, from at least 2015 through to this year.
- the hack of UK-US trade documents that were leaked ahead of the 2019 General Election – previously attributed to the Russian state via Written Ministerial Statement in 2020.
- the 2018 hack of the Institute for Statecraft, a UK thinktank whose work included initiatives to defend democracy against disinformation, and the more recent hack of its founder Christopher Donnelly, whose account was compromised from December 2021; in both instances documents were subsequently leaked.

- targeting of universities, journalists, public sector, non-government organisations and other civil society organisations, many of whom play a key role in UK democracy

Following a National Crime Agency investigation, the UK has today sanctioned two members of Star Blizzard for their involvement in the preparation of spear-phishing campaigns and associated activity that resulted in unauthorised access and exfiltration of sensitive data, which was intended to undermine UK organisations and more broadly, the UK government.

These sanctions have been delivered jointly with the US, and are the latest in our bilateral efforts to counter Russian malicious cyber activity that seeks to undermine our, and our allies', integrity and prosperity. The US Department of Justice have concurrently unsealed indictments against the individuals designated today.

The individuals being designated in the UK and US are:

- Ruslan Aleksandrovich PERETYATKO, who is a Russian FSB intelligence officer and a member of Star Blizzard AKA the Callisto Group
- Andrey Stanislavovich KORINETS, AKA Alexey DOGUZHIEV, who is a member of Star Blizzard AKA the Callisto Group

The Foreign, Commonwealth and Development Office has also summoned the Russian Ambassador to express the UK's deep concern about Russia's sustained attempts to use cyber to interfere in political and democratic processes in the UK and beyond.

In a statement to the House earlier today the Minister for Europe Leo Docherty emphasised that attempts to interfere with UK politics and democracy have not been successful. However, it is likely that Russia and other adversaries will continue to make attempts to use cyber means to interfere in UK politics. The NCSC alongside the US, Australia, New Zealand and Canada will today publish a cyber security advisory to inform network defenders of how to mitigate this activity, and NCSC will publish guidance for high-risk individuals whilst providing further information around support available.

Foreign Secretary David Cameron said:

> Russia's attempts to interfere in UK politics are completely unacceptable and seek to threaten our democratic processes.
>
> Despite their repeated efforts, they have failed.
>
> In sanctioning those responsible and summoning the Russian Ambassador today, we are exposing their malign attempts at influence and shining a light on yet another example of how Russia chooses to operate on the global stage.
>
> We will continue to work together with our allies to expose Russian covert cyber activity and hold Russia to account for its actions.

Deputy Prime Minister Oliver Dowden said:

> As I warned earlier this year, state actors, and the ‘Wagner-style’ sub-state hackers they use to do their dirty work, will continue to target our public institutions and our democratic processes.
>
> We will continue to call this activity out, to raise our defences, and to take action against the perpetrators.
>
> Online is the new frontline. We are taking a whole of society approach to ensuring we have the robust systems and cutting-edge skills needed to resist these attempts to undermine our democracy.

Home Secretary James Cleverly said:

> An attack against our democratic institutions is an attack on our most fundamental British values and freedoms. The UK will not tolerate foreign interference and through the National Security Act, we are making the UK a harder operating environment for those seeking to interfere in our democratic institutions.

The activity announced today is part of a broader pattern of malign cyber activity conducted by the Russian Intelligence Services across the globe. In recent years the UK and allies have exposed Russian Intelligence for their role in ViaSat, SolarWinds, and targeting of Critical National Infrastructure. In May, the NCSC alongside Five Eye partners exposed a sophisticated cyberespionage tool designed and used by Centre 16 of Russia’s Federal Security Service (FSB) for long-term intelligence collection on sensitive targets.

Background

These cyber-attacks were committed by a group NCSC assesses are highly likely subordinate to the FSB’s 18th Centre for Information Security. This is known in open source as:

- Star Blizzard
- SEABORGIUM
- Callisto Group
- TA446
- COLDRIVER
- TAG-53
- BlueCharlie
