Russia's FSB malign activity: factsheet

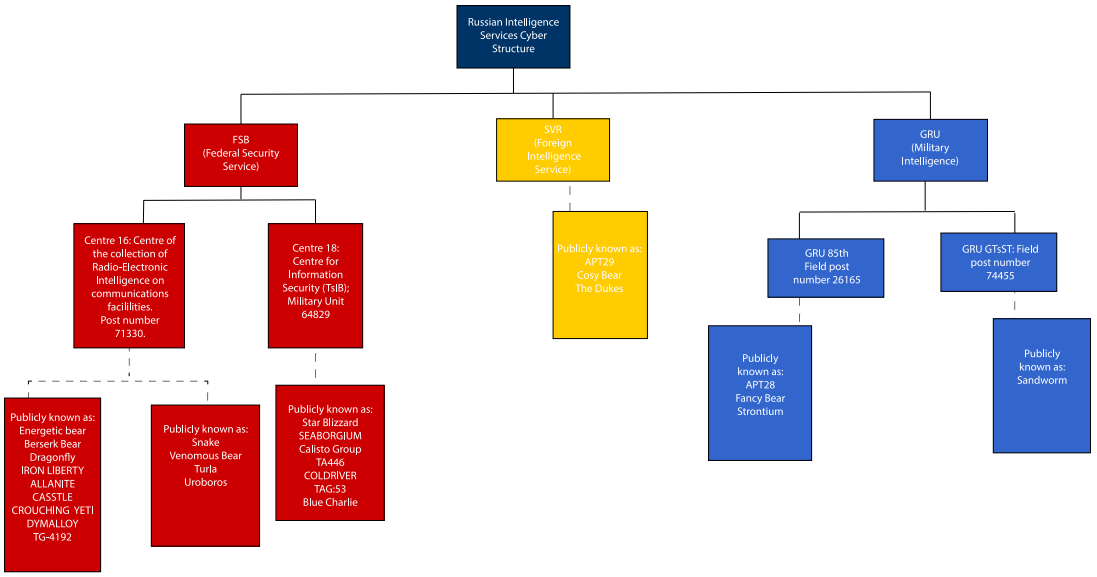
Archived: 2026-04-02 10:45:11 UTC

Cyber operations and the Russian intelligence services

Russia is one of the world's most prolific cyber actors and dedicate significant resource into conducting cyber operations around the globe. The UK government has publicly attributed malign cyber activity to parts of three Russian Intelligence services: the FSB, SVR and GRU, with each having their own remits.

A table of the parts of the Russian Intelligence Services that the UK Government has publicly attributed is below.

Russian Intelligence Services cyber organogram



Organogram showing the Russian Intelligence Services cyber structure.

Text alternative for the organogram: the Russin Intelligence Services Cyber Structure includes:

FSB (federal Security Service)

- Centre 16L Centre of the collection of radio-electronic intelligence on communications facilities, post number 71330. Publicly known as Energetic bear, Berserk Bear, Dragonfly, IRON LIBERTY, CASSTLE, CROUCHING YETI, DYMALLOY, TG-4192, Snake, Venomous Bear, Turla, Uroboros
- Centre 18: Centre for Information Security (TsIB), military unit 64829. Publicly known as: Star Blizzard, SEABORGIUM, Calisto Group, TA446, COLDRIVER, TAG:53, Blue Charlie

SVR (Foreign Intelligence Service), publicly known as APT29, Cosy Bear, The Dukes

GRU (Military Intelligence)

- GRU 85th, field post number 26165. Publicly known as APT28, Fancy Bear, Strontium
- GRU GTsST: field post number 74455. Publicly known as: Sandworm

The FSB cyber programme

The FSB (Federal Security Service; Russian: (Федеральная служба безопасности (ФСБ)) is Russia's state security agency and the successor to the KGB. Since its formation in (1995 the FSB has conducted electronic surveillance of equipment. The UK has exposed the involvement of 2 FSB Centres in cyber activity directed against the UK.

- Centre 16 supports Foreign Intelligence collection, as well as supporting the wider FSB mission (to include protection of the constitution)
- Centre 18 sits within the Counter-Intelligence Service of the FSB (Service 1)

FSB Centre 16

FSB Centre 16 (16-й Центр) is responsible for cyber operations including the intercepting, decrypting and processing of electronic messages, and the technical penetration of foreign targets. Its full title is the Centre for Radio-Electronic Intelligence by Means of Communication (TsRRSS; Russian: Центр радиоэлектронной разведки на средствах связи (ЦРРСС)) and is also known as "Military Unit 71330" (V/Ch 71330) (Войсковая часть В/Ч 71330).

When the KGB was disbanded in 1991, the 16th Directorate of the KGB became FAPSI (Russian: ФАПСИ) or Federal Agency of Government Communications and Information (FAGCI) (Russian :Федеральное Агентство Правительственной Связи и Информации), a Russian government agency, which was responsible for signals intelligence (SIGINT) and security of governmental communications.

In 2003, FAPSI was dissolved, and the 3rd Main Department of FAPSI (responsible for SIGINT) was transferred to the FSB forming the basis for FSB Centre 16.

The emblem of FSB Centre 16 hints at its activities in cyberspace: a satellite dish (signifying SIGINT activity) and a key, broken by lightning, (signifying the breaking of an encryption key) are both present.

Emblem of FSB Centre 16

Cyber operations conducted by FSB Centre 16

FSB Centre 16 has been observed conducting cyber operations since at least 2010. They conducted significant campaigns against the energy sector in 2014 and the aviation sector in 2020.

FSB Centre 16 is also responsible for snake malware and its variants which have been a core component in espionage operations conducted by Centre 16 for nearly 2 decades. The implant has been used to collect sensitive information from specific targets, such as government networks, research facilities and journalists, with Snake infrastructure identified in more than 50 countries across the world.

Cyber operations against worldwide critical national infrastructure

Centre 16 of the FSB have targeted/gained unauthorised access systems in countries around the world that are necessary for a country to function and upon which daily life depends. Known as Critical National Infrastructure or CNI, Centre 16 has targeted systems essential for energy, healthcare, finance, education and local/national governments. This has been a concerted campaign over many years and in a wide range of countries across Europe, the Americas and Asia.

The National Cyber Security Centre (NCSC) and cyber security companies have warned network defenders on multiple occasions of the risks posed by this pattern of activity. While there has been speculation of FSB involvement, the UK government is confirming this activity was carried out by FSB Centre 16 and providing further details of specific examples of this activity to increase awareness and transparency around the threat.

Table 1: Cyber operations against CNI

Date	Activity	Description of targets	Further information
June to July 2013	Compromised software package, turning the software into a Trojan, a legitimate appearing programme that contains malware	European manufacturer of programmable logic controller devices	Symantec report: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
April 2014	Compromised software	European developer of wind turbines, bio gas and other energy infrastructure	Symantec report: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
April 2017	Conducted malicious cyber activity	UK companies associated with the energy sector	
October 2017	Gained unauthorised access to and compromised	European and North American energy sector	Symantec report: Dragonfly: Western energy sector targeted by sophisticated attack group https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks. Symantec indicate that the actors may have “access to operational systems”

Date	Activity	Description of targets	Further information
	multiple networks through malicious cyber activity including spear phishing		
March 2018	Conducted spear phishing, captured user credentials, gained unauthorised access to CNI and exfiltrated data	US energy, nuclear, commercial facilities, water, aviation and critical manufacturing sectors	US Cybersecurity and Infrastructure security agency advisory https://www.cisa.gov/uscert/ncas/alerts/aa22-074a. [The advisory states that th activity detailed was performed by Russia government actors and points to the Symantec report detailed above (October 2017) that details malicious activity performed by the group called “Dragonfly”]
April 2018	Compromising UK organisations with focus on engineering and industrial control companies. Attackers may be able to access contact lists of hacked companies and establish long term access to networks	UK engineering and industrial control companies	NCSC advisory: https://www.ncsc.gov.uk/news/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control
February 2020 to August 2020	Sustained and substantial scanning and probing of networks	American aviation sector	This reconnaissance could be used to gain access at a later date
September 2020 onwards	Targeted and exfiltrated data	American aviation sector and other key US targets	CISA alert AA20-296A

Cyber operations against dissidents, political opponents and the Russian public

The UK government has identified FSB Centre 16 actors using cyber operations to monitor or attempt to gain unauthorised access to the computer systems of dissidents, political opponents and the Russian public.

Table 2: Cyber operations conducted by FSB Centre 16 against dissidents, prominent Kremlin critics and the Russian public

Date	Activity	Further information
September 2017	Gained unauthorised access to the email address of an associate of Aleksey Navalny	Aleksey Navalny is a prominent critic of Putin and a strong advocate for democracy in Russia. In August 2020 Navalny was poisoned in Russia. Following treatment in Germany he returned to Russia and was arrested on arrival
October 2019 to January 2020	Posing as the Russian Federal Tax Service, conducted spear phishing against multiple Russian nationals	Many of the targets are critics of the current administration
February 2020	Attempted to Spear-phish the press secretary of Mikhail Khodorkovskiy	1: Mikhail Khodorkovskiy is a prominent critic of the Russian administration and currently resides in the UK. 2: Mikhail Khodorkovskiy has said he believes himself to be at serious risk from harm at the hands of the Russian state. He currently resides in the UK. The press secretary would be expected to have access to Mikhail Khodorkovskiy's diary and travel plans
May 2020	Monitored the website "dossier.center", a website set up by Mikhail Khodorkovskiy to expose corruption within the Russian government. This activity occurred shortly after the website released information about the FSB	This activity likely represents intelligence gathering against groups connected to Mikhail Khodorkovskiy

FSB Centre 18

FSB Centre 18 is also known as the Centre for Information Security (TsIB) Military Unit 64829. Centre 18 sits within the FSB 1st Service (Counter-intelligence Service). NCSC assesses that Star Blizzard is almost certainly subordinate to the Russian Federal Security Service (FSB) Centre 18.

Star Blizzard have conducted cyber espionage operations targeting the UK, including key parts of the democratic and political process. The group have also selectively leaked and amplified the release of information in line with Russian information confrontation priorities, including to undermine trust in politics in the UK and likeminded states.

NCSC has warned of the risks posed by this pattern of activity, including in a technical advisory in January. While there has been speculation of FSB involvement, the UK government is confirming this activity was carried out by a group subordinate to FSB Centre 18 and providing further details of specific examples of this activity to increase awareness and transparency around the threat.

Emblem of FSB Centre 18

Table 3: Cyber operations conducted by Star Blizzard against high-profile UK political figures and organisations

Date	Activity	Further information
From at least 2015 to 2023	Targeting of UK Parliamentarians	Targeting of Parliamentarians from multiple, parties, including impersonation of individuals and spear-phishing attempts.
2018	Hack of the Institute for Statecraft	Hack of the institute for Statecraft, a UK thinktank whose work included initiatives to defend democracy against disinformation – the documents subsequently leaked.
2019	Hack of UK-US trade documents	The hack of UK-US trade documents that were leaked ahead of the 2019 UK General Election.
From December 2021	Hack of Institute for Statecraft founded Christopher Donnelly	The hack of Institute for Statecraft founder Christopher Donnelly – documents were subsequently leaked.

Source: https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet