



## BRIEFING PAPER

Number CBP 8430, 30 October 2018

# Russian intelligence services and special forces

By Ben Smith

**Contents:**

1. KGB reborn?
2. GRU
3. Spetsnaz
4. What's new?



# Contents

<b>Summary</b>	<b>3</b>
<b>1. KGB reborn?</b>	<b>4</b>
1.1 FSB	4
1.2 SVR	5
1.3 FSO and GUSP	5
<b>2. GRU</b>	<b>7</b>
Cyber warfare	7
NCSC Review	8
<b>3. Spetsnaz</b>	<b>9</b>
<b>4. What's new?</b>	<b>11</b>

## Summary

The Salisbury incident and its aftermath brought the Russian secret services into the spotlight. Malcolm Chalmers of [Royal United Services Institute](#) said Russian security services were going well beyond normal spying practice: “By launching disruptive operations that threaten life in target societies, they blur the line between war and peace”.

The main domestic service, the FSB, is a successor to the Communist-era KGB. It is responsible for counter-terrorism and counter espionage and Russian information security. Critics say that it continues the KGB’s work of persecution of ‘dissidents’ and is guilty of torture and other human rights violations, and of extortion and corruption.

One estimate put its staff complement at 200,000, and it has grown in power, particularly since the election of Vladimir Putin as President of Russia. Many senior Russian government officials and company heads are ‘siloviki’ – former members of the security services.

The SVR is the foreign intelligence service and was also formed from the remains of the KGB. It is known to have run a number of ‘illegals’: moles in foreign countries with false identities and no diplomatic cover. Anna Chapman, arrested in the US 2010, was a SVR spy.

There are other elements of the former KGB such as the FSO and the GUSP. Their role is to protect high government officials among other things but details of their work are not available.

The GRU is the military intelligence agency and is described as particularly audacious; its official remit is providing military intelligence to the Russian president and government, and ensuring Russia’s military, economic and technological security. The GRU has been behind many of the cyber attacks against Western institutions, including the one which resulted in a leak of emails from the US Democratic Party in 2016. In 2018, the investigative website Bellingcat released the names of 305 individuals it suspected of being GRU agents.

Spetsnaz are Russian special forces. They are trained in fighting but also in intelligence work and are attached to various military forces. The GRU has its own spetsnaz forces. Spetsnaz have been involved in conflicts including Afghanistan, Ukraine and Syria.

While the Kremlin seems to be pushing political intervention in rival states as a strategy, something known to the Soviets as ‘active measures’, the fact that so much of these operations has become public knowledge and so many of them have failed is perhaps surprising.

Western governments’ strategy of making public as much of what they know as possible is different to earlier thinking, whereby the secret services would keep their discoveries and methods as secret as possible.

# 1. KGB reborn?

The KGB was dismantled on the collapse of the Soviet Union but the GRU survived. Russia's two other main intelligence and security services were created from the remains of the KGB: the Foreign Intelligence Service, or SVR, and the Federal Security Service, or FSB, plus some other bodies.

## 1.1 FSB

The Russian Government describes the FSB as a:

...federal executive body with the authority to implement government policy in the national security of the Russian Federation, counterterrorism, the protection and defence of the state border of the Russian Federation, the protection of internal sea waters, the territorial sea, the exclusive economic zone, the continental shelf and their natural resources, ensuring the information security of Russia.<sup>1</sup>

The director is Alexander Bortnikov and the service is overseen by the President of the Russian Federation. "Cautious estimates" put the number of employees of the FSB at some 200,000.<sup>2</sup>

Vladimir Putin is a former KGB officer and is very close to the FSB and surrounds himself with other siloviki – politicians who used to be members of the security services. Vladimir Putin also extended the remit of the FSB, allowing it to take over many of the functions of the old KGB, including operating abroad and carrying out special operations.

Analysts argue that the siloviki have been in the ascendant in government circles at the expense of the oligarchs, the billionaire businessmen who control much of the economy.<sup>3</sup> In 2000, the Director of the FSB described his officers as "the new nobility".<sup>4</sup>

FSB officers have been accused of torture and other human rights violations.<sup>5</sup>

FSB officers are also allegedly involved in illicit income generation. According to the Kleptocracy Initiative, an anti-corruption NGO:

The FSB controls business activities in Russia through a complex system of practices, the most common of which is extorting businesses for money/kickbacks. When a businessman refuses to surrender his assets, or to "share" as it is called, it is not unusual for the FSB to dismantle and/or seize the company.<sup>6</sup>

---

<sup>1</sup> Russian Government, [Federal Security Service: Description](#),

<sup>2</sup> Andrei Soldatov and Irina Borogan, '[Russia's New Nobility](#)', *Foreign Affairs*, September/October 2010

<sup>3</sup> Karina Orlova, '[The siloviki coup in Russia](#)', *The American Interest*, 21 September 2016

<sup>4</sup> Andrei Soldatov and Irina Borogan, '[Russia's New Nobility](#)', *Foreign Affairs*, September/October 2010

<sup>5</sup> "[You should understand: FSB officers always get their way!](#)": Anti-fascist Viktor Filinkov reveals how he was tortured by Russian security services', OpenDemocracy, 28 February 2018

<sup>6</sup> '[Local Businessman, the FSB, and Corruption](#)', Kleptocracy Initiative, 25 August 2015

## 1.2 SVR

The SVR is the foreign intelligence service, mainly for civilian matters. It was formed from the Soviet-era KGB's first Chief Directorate after the fall of the Soviet Union.

It shares several functions with the GRU:

1. Political Intelligence.
2. Scientific and Technical Intelligence (industrial espionage).
3. Illegal Intelligence

It has one function that is not shared with the GRU: exterior counter-intelligence.<sup>7</sup>

Its head is Sergei Naryshkin. The service is overseen by the President of the Russian Federation.

A former US national counter-intelligence official said in 2016 that he believed that more than 100 agents of Russia's SVR foreign intelligence service were operating in the US,<sup>8</sup> after a significant ramping up of espionage operations.

Anna Chapman was one of a ring of SVR spies based in the US that was broken up in 2010; one of its responsibilities was to report on US elections, according to the US Intelligence Community.<sup>9</sup> 10 were arrested and exchanged for four other prisoners held by Russia. Among these were Sergei Skripal, former GRU official and victim of the nerve agent attack in Salisbury; and Igor Sutyagin, a former arms control researcher at a think tank in Moscow who always denied being a spy. He later worked with the Royal United Services Institute to publish the report about spetsnaz forces quoted below.

In 2015 allegations circulated that Gareth Williams, an employee of GCHQ and MI6, had been killed by SVR agents because he knew the identity of a Russian mole in GCHQ.<sup>10</sup>

## 1.3 FSO and GUSP

### FSO

The Federal Guard Service is another former element of the KGB and is comparable to the Metropolitan Police Protection Command, being responsible for protecting high ranking officials and important premises. According to a [1996 document posted by the Federation of American Scientists](#), the FSO:

...supervises top-level government communications, operates and protects underground command centers, maintains the special underground train system that connects key government facilities

---

<sup>7</sup> Konstantin Preobrazhensky, [GRU: Obscure Part Of Russian Intelligence](#), *Journal of Defense Management*, 26 March 2012

<sup>8</sup> ['Russian spies adopt new tactics to battle old enemy'](#), *Financial Times*, 14 December 2016

<sup>9</sup> [Assessing Russian Activities and Intentions in Recent US Elections](#), US Intelligence Community Assessment, January 2017, p5

<sup>10</sup> ['MI6 spy Gareth Williams was 'killed by Russia for refusing to become double agent'](#), former KGB man claims', *Independent*, 28 September 2015

## 6 Russian intelligence services and special forces

in the Moscow area, and protects other strategic facilities, and executive aircraft and special trains.

### **GUSP**

GUSP is the Main Directorate of Special Programmes of the President of the Russian Federation. According to the Russian Government the unit is:

...responsible for assisting the President, within its scope of competence, in exercising his powers in the sphere of mobilisation preparations and mobilisation of the bodies of state authority in the Russian Federation, ensuring coordination and interaction in their work and the work of federal and regional bodies of executive authority, as well as a failsafe functioning of the centres of governing the state and its Armed Forces, and security of the President, Prime Minister and other top officials.<sup>11</sup>

The director is Alexander Linets, who answers directly to the President of the Russian Federation.

---

<sup>11</sup> Russian Government, [Chief Directorate for Special Programmes of the Russian President](#)

## 2. GRU

Russia's military intelligence service is commonly known as the GRU, which stands for Main Intelligence Directorate in Russian.

Its published aims are providing military intelligence to the Russian president and government, and ensuring Russia's military, economic and technological security.

The GRU answers directly to the chief of the general staff, Valery Gerasimov, and the Russian defence minister, Sergei Shoigu.

The GRU is reported to specialise in running 'illegal' spies - those who work without diplomatic cover and who live under an assumed identity in the target country.

The GRU controls a large Spetsnaz (special purposes) force, reportedly numbering 25,000 in 1997.<sup>12</sup>

### Cyber warfare

It has a leading role in cyber warfare. and have been implicated in the cyber attacks on the US 2016 presidential election, the attempted murder of the Skripals, the attempted hacking the FCO and the Defence Science and Technology Laboratory (Porton Down), the World Anti-Doping Agency, the Organisation for the Prevention of Chemical Weapons (OPCW) and the Malaysia airlines MH-17 investigation.<sup>13</sup>

In January 2017 US intelligence community reported that the GRU was behind the Democratic Party email hacking:

The General Staff Main Intelligence Directorate (GRU) probably began cyber operations aimed at the US election by March 2016. We assess that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political figures. By May, the GRU had exfiltrated large volumes of data from the DNC.<sup>14</sup>

### 305 GRU suspects named

On 4 October 2018 the investigative journalism site Bellingcat announced that it had found the names and personal details of 305 individuals suspected of working for GRU, in what was described as the biggest blunder in Russian espionage since the end of the Cold War.<sup>15</sup> Like the Skripals suspects, information was in the public domain that linked them to the GRU: in this case car registration details.<sup>16</sup>

On the same day, a grand jury in the Western District of Pennsylvania has indicted seven alleged GRU officers for computer hacking, wire fraud, aggravated identity theft, and money laundering. The indictments

---

<sup>12</sup> Lunev, Stanislav ["Changes may be on the way for the Russian security services"](#). PRISM. The Jamestown Foundation. 12 September 1997

<sup>13</sup> ["What is Russia's GRU military intelligence agency?"](#), Reuters, 5 October 2018

<sup>14</sup> [Assessing Russian Activities and Intentions in Recent US Elections](#), US Intelligence Community Assessment, January 2017, p2

<sup>15</sup> 'How a Blunder Unmasked 305 Russian GRU Agents', *Voice of America*, 7 October 2018

<sup>16</sup> ["305 Car Registrations May Point to Massive GRU Security Breach"](#), Bellingcat, 4 October 2018

were particularly concerned with the hacking of the World Anti-Doping Agency.<sup>17</sup>

On 4 October 2018, the British and Dutch Governments issued a joint statement saying that the attack on the OPCW “demonstrates the GRU’s disregard for the global values and rules that keep us all safe”.

The statement went on:

Our action today reinforces the clear message from the international community: We will uphold the rules-based international system, and defend international institutions from those that seek to do them harm.<sup>18</sup>

## NCSC Review

The UK’s National Cyber Security Centre published its [2018 annual review](#) in October 2018, revealing that the majority of cyber attacks carried out in the UK came from groups sponsored or tolerated by hostile states, including Russia. It said, however, that there was “much, much more to the cyber security threat to the UK than just Russia”.

The NCSC says that the GRU is associated with the following hacking names:

- APT 28
- Fancy Bear
- Sofacy
- Pawnstorm
- Sednit
- CyberCaliphate
- Cyber Berkut
- Voodoo Bear
- BlackEnergy Actors
- STRONTIUM
- Tsar Team
- Sandworm<sup>19</sup>

---

<sup>17</sup> [‘U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations’](#), US Department of Justice press release, 4 October 2018

<sup>18</sup> [‘Joint statement from Prime Minister May and Prime Minister Rutte’](#), Downing Street press release, 4 October 2018

<sup>19</sup> [‘Reckless campaign of cyber attacks by Russian military intelligence service exposed’](#), National Cyber Security Centre press release, 4 October 2018



### 3. Spetsnaz

Spetsnaz are like a cross between US Rangers and the British SAS. They have a range of uses. They can fight but they are also trained for intelligence work. To establish insurgencies. To control them. To smuggle arms. To wage guerrilla wars.<sup>20</sup>

They are forces that can be inserted behind enemy lines or can maintain a low profile for long-term surveillance and reconnaissance missions. They also have a role as spearhead forces, clearing the way for less agile forces, relying on speed, stealth, and surprise to compensate for their lack of artillery and armour. Spetsnaz also focus on counter-insurgency operations and participate in the political sphere, participating in information warfare and what the Soviets used to call “active measures”.

There are several spetsnaz forces belonging to various military branches: ground forces, air forces and the Navy, although different authors use different definitions of ‘spetsnaz’.

One of the “most notorious” of spetsnaz units comes directly under the GRU.<sup>21</sup> The FSB internal security service also has a spetsnaz unit.

Every Russian reconnaissance brigade contains a spetsnaz component (roughly of battalion size) which conducts long range patrol and direct action.

Plans set out in 2013 projected the overall spetsnaz manpower of Russian conventional forces nearly doubling to the numbers shown in the table below:

#### Russian Special Operations Forces planned for 2018

	Brigades	Regiments	Battalions	Companies
GRU	7	1	4	0
Airborne Troops	1	0	0	9
Ground Troops	0	0	12	50
Total	8	1	16	59

Source: Igor Sutyagin, [Russia Confronts NATO: Confidence-Destruction Measures](#), RUSI, July 2016

There are seven regular spetsnaz brigades known as Independent Special Designation Brigades along with one other brigade (the 100th), the 25th Independent Special Purpose Regiment, and the forces attached to the new Special Operations Command.

Each brigade is made up of two or more regiments of approximately 500 personnel. Spetsnaz forces are further along the road to all-professional forces than most of the military; Some brigades are

<sup>20</sup> ‘Photos and roses for GRU’s ‘spetsnaz’ casualties’, *Financial Times*, 8 August 2014

<sup>21</sup> Christopher Marsh, [Developments in Russian Special Operations](#), CANSOFCOM Education and Research Centre, 2017

volunteer-only, while others have 20-30% conscripts.<sup>22</sup> They are elite units but analysts say they are not as proficient as some Western special forces.

### Operations

- Afghanistan

Spetsnaz forces struck inside Pakistan during the Afghan conflict.

- Chechnya

Now President Kadirov was in control of several spetsnaz units.

- Crimea

GRU spetsnaz forces took a leading role in the occupation of Crimea, storming the Crimean parliament. They later surrounded Simferopol airport and Belbek military airfield. Ukrainian border guards said that thousands of Russian troops arrived by military aircraft.<sup>23</sup>

- Ukraine

Six different spetsnaz brigades were involved in the Ukraine operation in its early stages. Memorials to 12 dead GRU spetsnaz members, killed in Ukraine, were displayed in a discreet ceremony in Moscow in 2014, despite official denials that any Russian forces were in Ukraine.<sup>24</sup> The spetsnaz deployment in mainland eastern Ukraine was more discreet than the Crimea deployment.

- Syria

Moscow has deployed Chechen and Ingush some 1,000 spetsnaz forces in Syria, who may operate more easily in that environment and whose loss would be less politically costly for the Russian Government than if they were ethnic Russians.

---

<sup>22</sup> Mark Galeotti, [The rising influence of Russian special forces](#), *Jane's Intelligence Review*, 2014

<sup>23</sup> ['Ukraine crisis: Pretext and plotting behind Crimea's occupation'](#), *Financial Times*, 7 March 2014

<sup>24</sup> ['Photos and roses for GRU's 'spetsnaz' casualties'](#), *Financial Times*, 8 August 2014

## 4. What's new?

Russian intelligence services have revived the Soviet-era strategy of 'active measures'. While gathering intelligence on Western politics or infrastructure, for example, could be classed as traditional spying, hacking the Democratic National Committee's emails and releasing them is intervening directly in the affairs of another state with a view to changing the course of events.

While the Kremlin's pursuit of active measures has probably strengthened in recent years, one puzzle is why so many agents have allegedly been unmasked by European intelligence services and the news media.

Is the obviousness deliberate? According to one analyst it could be:

...the exposure of several consecutive European operations should raise questions about whether Russian military intelligence is being intentionally provocative or has simply gone off the rails.<sup>25</sup>

According to several experts, the Kremlin is not overly concerned about the revelations. Mark Galeotti of the European University Institute said:

Not getting caught is not at the top of their priorities. The guidance from the Kremlin to the GRU is 'Get the job done, don't worry about the political costs'.<sup>26</sup>

Not getting caught might not be such a problem, then, since it could be to the Kremlin's advantage for the wide reach of its intelligence services to be just as widely known.

Failing to get the job done, as was the case with the Skripals, the attempts to hack the OPCW, the FCO and the MH17 investigation, can't be interpreted as a strategy.

A Russian security expert said the revelations were signs of a system "already in degradation":

Obviously they are worried about a whole series of reputational and organisational lapses, but there is definitely no sense of panic. The mistakes they made talk of a system in degradation, though that was already clear 10 years ago when Litvinenko was killed.<sup>27</sup>

### **New tactics**

For Western agencies to reveal so much of what they knew about the Russian agents was unusual and could be a disadvantage.

Commentators suggest that the Russian intelligence agencies will no longer be issuing passports with sequential numbers to their agents, for example, and are looking for officials who leaked information.

A British official explained the new tactic of revealing discoveries:

Shock went around the world after the novichok incident in Salisbury. We said we would call them out both to deter and to

---

<sup>25</sup> Andrew Roth, '[String of own goals by Russian spies exposes a strange sloppiness](#)', *Guardian*, 5 October 2018

<sup>26</sup> '[Bungling Russian spies will not worry the Kremlin](#)', *Financial Times*, 6 October 2018

<sup>27</sup> '[Salisbury suspects: Russian security services chase for 'leaks' after series of intelligence blunders](#)', *Independent*, 25 September 2018

## 12 Russian intelligence services and special forces

defend. We are not seeking to escalate, but we will defend ourselves, partly by shining a light and partly by sharing the information we have in a new way.<sup>28</sup>

Whether Western agencies' new strategy of shining a light on Russian agents will deter the Kremlin from its activities remains to be seen. At least they signal intent on the part of Western governments to take action.

---

<sup>28</sup> ['Bungling agents leave Putin exposed in the global spotlight'](#), *Guardian*, 4 October 2018

### About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email [papers@parliament.uk](mailto:papers@parliament.uk). Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email [hcenquiries@parliament.uk](mailto:hcenquiries@parliament.uk).

### Disclaimer

This information is provided to Members of Parliament in support of their parliamentary duties. It is a general briefing only and should not be relied on as a substitute for specific advice. The House of Commons or the author(s) shall not be liable for any errors or omissions, or for any loss or damage of any kind arising from its use, and may remove, vary or amend any information at any time without prior notice.

The House of Commons accepts no responsibility for any references or links to, or the content of, information maintained by third parties. This information is provided subject to the [conditions of the Open Parliament Licence](#).