The spies who came in from the Cold War

In their recently published annual reports, the Dutch intelligence and security services AIVD and MIVD note that the intelligence services of other countries often play a key role in covert influencing operations. These organisations either target political decision-making directly or focus on the manipulation of public perceptions indirectly. One of the countries mentioned with regard to these kinds of activities is

---

Russia. This country has long been most adept at covertly influencing the perceptions and public opinion in other countries, which can have a disruptive effect on policy-making processes. However, as they are carried out covertly, these activities have tended to remain hidden in the shadows. Lately though, they seem unable to stay out of the limelight. Recent operations by Russia’s intelligence services, in particular the military intelligence service GRU, are a case in point. Rarely has an intelligence service of a major power received so much public attention over such a short period of time as the GRU.

---

**Hacker, poisoner, soldier, spy**

One of the most prominent cyber cases to date was the use of the so-called Advanced Persistent Threat 28 – aka Fancy Bear – hack group to meddle in the 2016 US presidential election. According to the report by US Special Counsel Robert Mueller, twelve Russian intelligence officers from the GRU were guilty of hacking into the Democratic National Committee administration and the campaign for presidential candidate Hillary Clinton. Mueller’s findings fitted a clear pattern in which the GRU was found by the National Cyber Security Centre in the UK to be almost certainly responsible for an increasing number of cyber incidents in past years.

In another prominent case, the confidential medical files of a number of international athletes were released after a hack of the World Anti-Doping Agency’s administration and management system. And in April 2018, the GRU attempted to gain access to the computer networks of the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague. This was followed in May 2018 by a spear-phishing attempt in which the GRU’s hackers impersonated federal authorities in Switzerland to target OPCW employees, and thus again the...

---


OPCW’s computer networks. Recently, American intelligence contractor Booz Allen Hamilton published a report detailing all cyber operations carried out by GRU hackers over a period of 15 years, linking them to more than 200 espionage, disruption and disinformation incidents and campaigns in 33 separate case studies. Booz’s findings mirror those made earlier by the cyber security firm Symantec in 2018.

The GRU also played an important role in the annexation of Crimea in 2014 and in the instigation of separatism in Eastern Ukraine that followed. A GRU officer also played a key role in the shooting down of flight MH17 over Eastern Ukraine, also in 2014. Over the years the GRU has demonstrated a willingness to develop and sponsor paramilitary organisations that further Russian national interests. This trend has increased since the 2014 crisis in Eastern Ukraine, where the Kremlin used many of these paramilitary organisations to fight in the Donbass. The Russian government has also used private military companies such as the Wagner Group, consisting of a cadre of skilled operatives from GRU Spetsnaz, in a variety of non-attributable actions wherever and whenever required.

Finally, the attempted assassination of Sergei Skripal and his daughter in Salisbury in 2018 with a military nerve agent from the Novichok group again raised suspicions about the GRU, mainly because Skripal himself worked for the GRU when he was recruited by the British intelligence service MI6. The Skripal poisoning apparently served the combined purpose of sending a political message to the West and underscoring a continuing Russian campaign against traitors.

A life spent in the shadows

At present, there are three main intelligence and security services in Russia: the foreign intelligence service (SVR), the federal security service (FSB) and the military intelligence service (GRU). The latter has existed for the longest time. The acronym stands for Главное Разведывательное Управление (English: Main Intelligence Directorate) of the general staff of the armed forces, and as such the organisation falls within the responsibility of the Ministry of Defence. Of the various Russian intelligence services, and despite its recent level of activity, it is striking to note how little is known about the GRU compared to the Soviet KGB and its successor organisations SVR and FSB.

After the end of the Cold War and the dissolution of the Soviet Union, many former KGB officers and defectors wrote their memoirs, making information about the KGB accessible to a wider audience. The GRU, on the other hand, has always remained much more of a closed organisation.

One indication of this is that the number of significant memoirs written by ex-employees is negligible. Former KGB archivist Vasili Mitrokhin, together with British historian Christopher Andrew, has written a very comprehensive, two-volume standard work on the intelligence operations of the KGB in the Cold War. No such work on the GRU is available, however. But the fact that this intelligence service has become so ubiquitous as the tool through which Russia’s covert influencing operations are conducted warrants further scrutiny, not only by our own intelligence services but also by the decision-makers and publics targeted by it.


About the Clingendael Institute
Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

About the author

Danny Pronk is a Senior Research Fellow at Clingendael. His research focuses on security and defence issues, particularly in relation to China and Russia, and on geopolitical trend analysis, horizon scanning and strategic foresight.