Clingendael

Netherlands Institute of International Relations

Clingendael Alert

Danny Pronk

MAY 2020

The spies who came in from the Cold War

President Putin at a gala event dedicated to the 100th anniversary of the formation of the Main Directorate of the General Staff of the Armed Forces of Russia. Source: Kremlin.ru

Doing Russia's dirty work

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.[1] One of the countries mentioned with regard to these kinds of activities is

1 General Intelligence and Security Service (AIVD), Annual Report 2019, 29 April 2020, accessed 30 April 2020, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2019; Defence Intelligence and Security Service (MIVD), Annual Report 2019, 30 April 2020, accessed 30 April 2020, https://www.defensie.nl/downloads/jaarverslagen/2020/04/30/jaarverslag-mivd

Russia.[2] 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.[3] 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.[4]

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.[5] 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.[6]

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.[7] 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.[8] 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

2 See Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (London and New York: Routledge, 2019); Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Washington, DC: Georgetown University Press, 2019); and also Ivo Jurvee, "The Resurrection of 'Active Measures': Intelligence Services as a Part of Russia's Influencing Toolbox", *Hybrid CoE Strategic Analysis*, April 2018, accessed 24 April 2020, https://www.hybridcoe.fi/publications/strategic-analysis-april-2018-resurrection-active-measures-intelligence-services-part-russias-influencing-toolbox/

3 See Ladislav Bittman, "Soviet Bloc 'Disinformation' and other 'Active Measures'", in: Robert Pfaltzgraff, Uri Ra'anan and Warren Millbert (eds), *Intelligence Policy and National Security* (London: MacMillan Press, 1981), pp. 212-228; Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider's View* (Washington, DC: Pergamon-Brassey's, 1985); David V. Gioe, Richard Lovering and Tyler Pachesny, "The Soviet Legacy of Russian Active Measures: New Vodka from Old Stills?", *International Journal of Intelligence and Counterintelligence*, published online: 5 March 2020, pp. 1-26; Joseph S. Gordon, "Introduction", in *Psychological Operations: The Soviet Challenge*, edited by Joseph S. Gordon (London: Westview Press, 1988); Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (Washington, DC: Pergamon-Brassey's, 1984); Herbert Romerstein, "Disinformation as a KGB Weapon in the Cold War", *Journal of Intelligence History*, Vol. 1, No. 1 (2001), pp. 54–67.

4 Sergei Boeke and Ben de Jong, "Heads Rolling at the GRU? Blundering Russian Intelligence", *Clingendael Spectator*, 23 October 2018, accessed 23 April 2020, https://spectator.clingendael.org/en/publication/heads-rolling-gru-blundering-russian-intelligence; Christian Esch, "The Rise of Russia's GRU Military Intelligence Service", *Der Spiegel*, 19 October 2018, accessed 30 April 2020, https://www.spiegel.de/international/world/russia-and-the-rise-of-gru-military-intelligence-service-a-1233576.html

5 Special Counsel Robert S. Mueller, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* (Washington, DC: US Department of Justice, 2019).

6 National Cyber Security Centre, "Reckless campaign of cyber-attacks by Russian military intelligence service exposed", 3 October 2018, accessed 23 April 2020, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

7 Nicole Perlroth and Tariq Panja, "Microsoft Says Russians Hacked Antidoping Agency Computers", *The New York Times*, 28 October 2019, accessed 24 April 2020, https://www.nytimes.com/2019/10/28/sports/olympics/russia-doping-wada-hacked.html

8 Huib Modderkolk, *Het is oorlog, maar niemand die het ziet* (Amsterdam: Podium b.v. Uitgeverij, 2019); Militaire Inlichtingen- en Veiligheidsdienst, *Vooruitziend Vermogen voor Vrede en Veiligheid: Openbaar Jaarverslag 2018*, April 2019.

OPCW's computer networks.[9] 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.[10] Booz's findings mirror those made earlier by the cyber security firm Symantec in 2018.[11]

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.[12] 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.[13]

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.[14] The Skripal poisoning apparently served the combined purpose of sending a political message to the West and underscoring a continuing Russian campaign against traitors.[15]

9 David V. Gioe, "Cyber Operations and Useful Fools: The Approach of Russian Hybrid Intelligence", *Intelligence and National Security*, Vol. 33, No. 7 (2018), pp. 954–973.

10 Booz Allen Hamilton, *Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations*, 27 March 2020, accessed 6 April 2020, https://boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/bearing-witness-uncovering-the-logic-behind-russian-military-cyber-operations-2020.pdf

11 Symantec, "APT28: New Espionage Operations Target Military and Government Organizations", 4 October 2018, accessed 23 April 2020, https://symantec-enterprise-blogs.security.com/blogs/election-security/apt28-espionage-military-government

12 Kevin G. Hall, "Russian GRU Officer Tied to Downing of Passenger Plane in Ukraine", *Miami Herald*, 25 May 2018, accessed 24 April 2020, https://www.miamiherald.com/latest-news/article211871689.html ; Bellingcat, "Identifying the Elusive 'Elbrus': From MH17 To Assassinations In Europe", 24 April 2020, accessed 25 April 2020, https://www.bellingcat.com/news/uk-and-europe/2020/04/24/identifying-fsbs-elusive-elbrus-from-mh17-to-assassinations-in-europe/

13 Tor Bukkvoll and Åse G. Østensen, "The Emergence of Russian Private Military Companies: A New Tool of Clandestine Warfare", *Special Operations Journal*, Vol. 6, No. 1 (2020), pp. 1-17; Daniel Brown, "3 countries where Russia's shadowy Wagner Group mercenaries are known to operate", *Business Insider*, 27 April 2018, accessed 23 April 2020, https://www.businessinsider.nl/russia-wagner-group-mercenaries-where-operate-2018-4/?international=true&r=US ; Alexander Rabin, "Diplomacy and Dividends: Who Really Controls the Wagner Group?", *Foreign Policy Research Institute*, 4 October 2019, accessed 23 April 2020, https://www.fpri.org/article/2019/10/diplomacy-and-dividends-who-really-controls-the-wagner-group/ ; Matthew Cole and Alex Emmons, "Erik Prince Offered Lethal Services to Sanctioned Russian Mercenary Firm Wagner", *The Intercept*, 13 April 2020, accessed 23 April 2020, https://theintercept.com/2020/04/13/erik-prince-russia-mercenary-wagner-libya-mozambique/

14 David Omand, "From Nudge to Novichok: The Response to the Skripal Nerve Agent Attack Holds Lessons for Countering Hybrid Threats", *Hybrid CoE Working Paper*, April 2018, Accessed 24 April 2020, https://www.hybridcoe.fi/publications/nudge-novichok-response-skripal-nerve-agent-attack-holds-lessons-countering-hybrid-threats/; Mark Urban, *The Skripal Files: The Life and Near Death of a Russian Spy* (New York: Henry Holt and Company, 2018).

15 Luke Harding, *A Very Expensive Poison: The Definitive Story of the Murder of Litvinenko and Russia's War on the West* (London: Faber & Faber, 2016); David V. Gioe, Michael S. Goodman and David S. Frey, "Unforgiven: Russian Intelligence Vengeance as Political Theatre and Strategic Messaging", *Intelligence and National Security*, Vol. 34, No. 4 (2019), pp. 561–575; Amy Knight, *Orders to Kill: The Putin Regime and Political Murder* (London: Biteback Publishing, 2018).

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 *Glávnoye Razvedyvatel'noje Upravléniye* (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.[16] 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.[17] 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.[18] No such work on the GRU is available, however.[19] 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.

16 For instance Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations From Lenin to Gorbachev* (London: Hodder & Stoughton, 1990); Ben Macintyre, *The Spy and the Traitor* (London: Penguin, 2018); Pavel Sudoplatov and Anatoli Sudoplatov, *Special Tasks: The Memoirs of an Unwanted Witness, A Soviet Spymaster* (Boston: Little Brown & Co, 1994). Also Ben de Jong, *Schild en zwaard van de Oktoberrevolutie: De memoires van Sovjet inlichtingenofficieren, 1953-1991* (Maastricht: Shaker Publishing, 2004).

17 The only one being Viktor Suvorov, *Inside Soviet Military Intelligence* (London: Macmillan Publishing, 1984).

18 Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London and New York: Allen Lane, 2000); Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive II: The KGB and the World* (London and New York: Allen Lane, 2005).

19 The closest is Jonathan Haslam, *Near and Distant Neighbours: A New History of Soviet Intelligence* (Oxford and New York: Oxford University Press, 2015).

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

@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Newsletter

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.