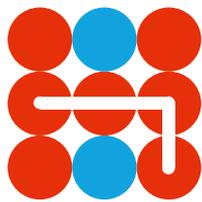

Strategic Analysis April 2018

The resurrection of ‘active measures’: Intelligence services as a part of Russia’s influencing toolbox

IVO JUURVEE



Hybrid CoE

The resurrection of ‘active measures’: Intelligence services as a part of Russia’s influencing toolbox

Russia’s Intelligence Services (RIS) are a key instrument in the country’s toolbox of hostile influence exerted abroad. As such, they are no mere ad hoc arrangement by some spy chief, nor a paranoid delusion of the West, but rather an integral function in accordance with Russian legislation and based on a long tradition. Indeed, their activities have extended far beyond information-gathering for the purpose of Russia’s decision-making. – writes Ivo Juurvee, Head of Security & Resilience Programme and Research Fellow at the International Centre for Defence and Security

The term ‘active measures’ became widely known in the Western academic and public discussion as early as the Cold War and is still sometimes used, although it has acquired many meanings that are not conveyed in the Russian discourse, and which may be confusing. Hence, a short excursion into the RIS, their functions and parlance is in order. Although possible assassinations by the RIS have been widely discussed since the poisoning of Sergei Skripal and his daughter in March 2018, this paper only deals with non-violent means of influencing. These are by far more common in peacetime and should not be overshadowed by single acts of violence.

There are three main intelligence services in Russia (collectively referred to as the RIS in this article): the Foreign Intelligence Service (SVR), the Federal Security Service (FSB), and the Military Intelligence (known as the GRU, but excluded here since its peacetime activities remain largely unknown). Together, they

form an integral part of the executive power in the Russian state apparatus.

The Russian definition of ‘intelligence activity’

Publicly available legislation defines the functions of the SVR and FSB. An article in the Federal Law on Foreign Intelligence of 1996 (originally regulating SVR action only, but with the 2003 Law on the Federal Security Service its scope was widened to the FSB as well) provides a two-part definition of ‘intelligence activity’. **The first part deals with the procurement and processing of information, which are classic intelligence service functions. The second part – support of the measures implemented by the state in order to ensure the security of the Russian Federation – is less explicit.** However, it is the original source of the abbreviation MS (*meropriyatiya sodeistviya* in Russian, or ‘support measures’) used in the name of a unit in both the SVR and FSB.



What does the term support measures mean and where does it originate from?

Public sources do not provide an answer. The term already appeared in the 1992 version of the Law on Foreign Intelligence, probably written by the former offices of the KGB (the Soviet intelligence and security service) and based on its experience.

The KGB's once top-secret definition of intelligence was among the reams of notes smuggled to Britain by the defecting senior KGB archivist Vasili Mitrokhin and is now known: A secret form of political struggle which makes use of clandestine means and methods for acquiring secret information of interest and for carrying out active measures to exert influence on the adversary and weaken his political, economic, scientific and technical and military positions.

Comparing the two terms, intelligence activity and support measures, we can draw the conclusion (corroborated by SVR defector Sergei Tretyakov) that support measures are the direct successors of active measures, and merely a new and politically correct term formulated after the fall of the Soviet Union. It is also worth noting that when President Vladimir Putin and other ex-KGB officers in the current Russian leadership received their education in the KGB's academies, intelligence was defined as a 'secret form of political struggle'.

Support measures can be studied through the substance of the Cold War active measures concept

Since the current RIS handbooks on support measures are unavailable for scrutiny

for obvious reasons, it is worth taking a closer look at the abundance of material on the essence of active measures. These were defined by the KGB as *agent-operational measures aimed at exerting useful influence* on a wide variety of subjects in the political life of the target country.

As known from documents provided by defectors, these measures were generally directed towards sowing discord between the allies, and were frequently concerned with undermining the United States, although they sometimes had the narrower operational goal of discrediting a particular person. The use of agents was not absolutely necessary, as the measures also involved mailing copies of authentic or forged documents (the antecedents of 'fake news') and articles to the media and political establishment promoting views similar to the Kremlin's. The internet has changed the technical modus operandi completely, however, as such work can now be executed far more cheaply and with no need for the direct involvement of the RIS.

Agent of influence and confidential contacts as tools for active measures in the Soviet Union

Delving deeper, the term **agent of influence** was also used, namely: ***an agent operating under intelligence instructions who uses his official or public position, and other means, to exert influence on policy, public opinion, the course of particular events, the activity of political organizations, and state agencies in target countries.*** Such people were not only operating under intelligence instructions but also clearly aware of their deeds, and in receipt of (usually financial) benefits for their work in the interests of Moscow. The public position implied that any kind of opinion leader could be re-



cruited. However, in the field of influence operations, the KGB's main strength did not reside in agents, but in **confidential contacts: individuals of foreign nationality who, without being agents, communicate to intelligence officers information of interest to them and carry out confidential requests**, which in substance are of an intelligence nature, and based on ideological and political affinity, material interest, and friendly or other relations that they have established with intelligence officers. Confidential contacts worked on a voluntary basis and had no obligations towards intelligence officers.

These designated agents of influence and confidential contacts may have been easy to detect, but almost impossible to convict in a democratic country. **Providing classified information to foreign powers is penalized in every country and the perpetrators may be caught red-handed with evidence (usually copies of classified documents or some kind of digital traces of having smuggled them). However, disseminating the Kremlin's talking points or facilitating its agenda is not a crime, especially if it is performed out of 'ideological and political affinity'.** Confidential contacts can claim – and sometimes truly believe – that they are communicating with ordinary Russian diplomats or just friendly Russians, not RIS officers. It is logical to assume that at least some of the persons labelled as useful idiots (a term probably wrongly attributed to Lenin) may appear as confidential contacts in current RIS files. Without having direct access to RIS documents or information from defectors, it is virtually impossible for counter-intelligence to differentiate between agents of influence and confidential contacts. The difference between confidential

contacts and useful idiots is even more blurred.

The information-gathering capacity of the RIS is key. Without in-depth knowledge and facts, conducting efficient support measures is difficult. **For example, in order to magnify distrust in society, there has to be knowledge about existing polarization and the reasons behind it. When seeking to discredit a person, their personal information has to be acquired. This means that information, any information, has value.** The growing number of Russian spies detained and convicted abroad compared to earlier decades indicates that human intelligence (HUMINT) is being actively deployed. However, the link between HUMINT and support measures is difficult to prove from open sources.

A case occurred in March 2014 in which a phone conversation between the EU High Representative of the Union for Foreign Affairs and Security Policy and the Estonian Minister of Foreign Affairs was tapped, uploaded to YouTube and clips from it instantly used by RT (formerly Russia Today), a Russian TV network targeted at an international audience. Although the eavesdropper was never identified, the RIS would seem to be the only entity possessing both the signals intelligence capacity and the intent to use it in the interests of the Russian media during the intense phase of the Ukraine crisis. **This case and similar ones highlight the issue of using information procured by the RIS for media operations. Information collected by the RIS can also contribute to better planning of information influence operations and provide feedback on their outcome. It may also be used as a basis for diplomatic and economic efforts to influence political decisions abroad.**

Russian intelligence service activities abroad will not disappear

RIS activities abroad, support measures included, will not disappear in the foreseeable future. **The expulsion of alleged RIS officers after the Skripal poisoning case may have a containment effect in several countries, but the RIS will have the possibility to use its assets in third countries or to intensify its activities from Russian territory.** The use of such options is highly likely, especially if diplomatic means become ineffectual in the face of escalating tensions.

This is not to say that there is no way to effectively counter their work. **In the field of legislation and law enforcement, attention should turn to the issue of agents of influence, and confidential contacts in particular.** This is a hard nut to crack for legislators. However, elaborating and properly enforcing current laws on tax evasion and money laundering, and making lobbying activities more transparent would curtail the way in which agents of influence and confidential contacts operate. **An important measure entails exposing the RIS modus operandi in influence activities.** In the past, educating the public has proved to be an efficient way of raising awareness and duly minimizing the impact of such activities. One way of raising awareness, as exemplified during the Cold War, is the publication of memoirs or books by Rus-

sian/Soviet intelligence defectors. Memoirs contain important empirical information on the field of influence activities. The most recent memoirs by an RIS defector were published more than a decade ago, and while memoirs might be obsolete as a genre, similar information-sharing would be especially helpful for diplomats, politicians, journalists, academics, think tankers, and even the public at large.

When it comes to signals intelligence and the cyber domain, the question of data protection becomes crucial. Governments are already making great efforts to protect classified information. However, political parties, NGOs, opinion leaders and even ordinary citizens still have their work cut out in terms of IT security. Any type of leak or hacking operation can be exploited by the RIS and funnelled to Russian propaganda channels. Finally, it goes without saying that top-notch counter-intelligence work is essential for countering measures.

The RIS is an integral part of the executive power in Russia (not a state within a state having tasks antagonistic to other elements of power). According to Russian legislation, they are compelled to take part in the 'political struggle' by the clandestine means available to them. Hence, it is reasonable to assume that in this respect the legislation in Russia will be honoured. To this end, influence activities by the RIS will remain a persistent problem in the future.



Author

Dr. **Ivo Juurvee** is Head of Security & Resilience Programme / Research Fellow at the International Centre for Defence and Security (ICDS). He has been a practitioner in the field of security for more than 13 years. Among other positions in the Estonian public service, he has served as an adviser at the National Security and Defence Coordination Unit of the Estonian Government Office. Prior to joining ICDS in 2017, he worked as the head of the Internal Security Institute of the Estonian Academy of Security Sciences (EASS). Dr. Juurvee has also taught security-related topics at the University of Tartu, the NATO School at Oberammergau, and on the FRONTEX master's programme on border management. He has worked as an Honorary Research Fellow at University College London's School of Slavonic and East European Studies. As part of the ICDS team, Dr. Juurvee focuses on security and resilience, namely the countermeasures applicable to the wide spectrum of threats to Estonia and more widely to NATO and the EU. These include: intelligence/counter-intelligence, terrorism/counter-terrorism, information warfare/psychological defence, and other means of non-conventional foreign pressure and the national resilience required to cope with them.

Literature:

Pete Earley. *Comrade J: the untold story of Russia's master spy in America after the end of the Cold War*. New York: G. P. Putnam's Sons, 2007.

Mark Galeotti. *Putin's hydra: Inside Russia's intelligence services*. ECFR, 2016. http://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services.

Ivo Juurvee. *Spy Swaps Make a Comeback in "Intelligence Culture"*. ICDS Blog, 2018. <https://www.icds.ee/blog/article/spy-swaps-make-a-comeback-in-intelligence-culture/>.

Edward Lucas. *Deception: Spies, Lies and How Russia Dupes the West*. London: Bloomsbury, 2012.

Juha Mustonen, Aapo Cederberg, Pasi Eronen. *Regional Cooperation to Support National Hybrid Defence Efforts*. HybridCoE, 2017. https://www.hybridcoe.fi/wp-content/uploads/2017/12/hybridcoe_wp1_regional_cooperation.pdf

Andrei Soldatov, Irina Borogan. *The New Nobility: The Restoration of Russia's Security State and Enduring Legacy of the KGB*. New York: Public Affairs, 2010.

Documents made available by KGB defectors

Christopher Andrew, Oleg Gordievsky (eds.) *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975–1985*. London: Sceptre, 1993.

Christopher Andrew, Oleg Gordievsky (eds.) *More Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975–1985*. London: Frank Cass, 1992.

Vasily Mitrokhin (ed.) *KGB Lexicon: The Soviet Intelligence Officers Handbook*. London: Routledge, 2002.

GBR/0014/MITN – The Papers of Vasily Mitrokhin, available at the Churchill Archives Centre in Cambridge.

Russia's laws

Federal Law on Foreign Intelligence (1992) <http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102017351&back-link=1&nd=102017360&rdk=0>.

Federal Law on Foreign Intelligence (1996) <http://ivo.garant.ru/#/document/10135745/paragraph/19:0>.

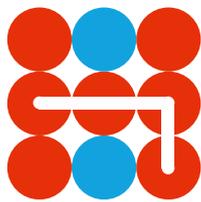
Federal Law on Federal Security Service (1995) <http://www.fsb.ru/fsb/npd/more.htm%21id%3D10340801%40fsbNpa.html>.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-07-6

Hybrid CoE is an international hub for practitioners and experts, building member states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

The responsibility for the views expressed ultimately rests with the authors.



Hybrid CoE