

Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?

FREDRIK WESTERLUND



Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?

In 2010, it was not so much a question of whether the intelligence services of the Russian Federation would support domestic science and industry as of how effective they would be in doing so. The multiple Russian intelligence services had been gathering foreign scientific and technological know-how for many years as well as providing security and, to some extent, managerial support to Russian industry.

There were, however, problems with successfully transferring the foreign technology acquired, and there were obvious hazards involved alongside the benefits of employing intelligence services to further national science and industry. Even though support from the intelligence services may seem like a promising short cut to Russian modernisation, it could in the long run turn out to be a dead end.

In this report, the current situation in Russia is reviewed through the study of historical precedents, contemporary official documents and assessments by professionals in the field of intelligence. The author explores the opportunities for, as well as the obstacles to and risks connected with, intelligence service support to national science and industry in a contemporary Russian context.

This report is available in PDF-format on the FOI Russia Research Project website: <http://www.foi.se/rufs>

Fredrik Westerlund

Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?

On the cover page The GRU emblem (left), the SVR emblem (centre) and the FSB emblem (right) on the Russian Federation flag

Titel	Rysk underrättelseinhämtning för inhemsk FoU – en genväg eller återvändsgränd i modernisering?
Title	Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?
Rapportnr/Report no	FOI Memo 3126
Rapporttyp/Report Type	Memo
Månad/Month	April
Utgivningsår/Year	2010
Antal sidor/Pages	45 p
ISSN	
Kund/Customer	Försvarsdepartementet/Department of Defence
Projektnr/Project no	A12001
Godkänd av/Approved by	Eva Mittermaier
FOI, Totalförsvarets Forskningsinstitut	FOI, Swedish Defence Research Agency
Avdelningen för Försvarsanalys	Division of Defence Analysis
164 90 Stockholm	SE-164 90 Stockholm

Summary

In 2010, it was not so much a question of whether the intelligence services of the Russian Federation would support domestic science and industry as of how effective they would be in doing so. The multiple Russian intelligence services had been gathering foreign scientific and technological know-how for many years as well as providing security and, to some extent, managerial support to Russian industry.

There were, however, problems with successfully transferring the foreign technology acquired, and there were obvious hazards involved alongside the benefits of employing intelligence services to further national science and industry. Even though support from the intelligence services may seem like a promising short cut to Russian modernisation, it could in the long run turn out to be a dead end.

In this report, the current situation in Russia is reviewed through the study of historical precedents, contemporary official documents and assessments by professionals in the field of intelligence. The author explores the opportunities for, as well as the obstacles to and risks connected with, intelligence service support to national science and industry in a contemporary Russian context.

Keywords: Russia, Russian Federation, intelligence services, security services, science, technology and industry, research and development (R&D), innovation, modernisation.

Sammanfattning

I slutet på det 21 århundradets första decennium var det inte fråga om ryska underrättelse- och säkerhetstjänster skulle stödja inhemsk forskning och industri, utan snarare hur effektivt ett sådant stöd skulle kunna vara. Ryska underrättelsetjänster hade sedan många år tillbaka inhämtat vetenskaplig och teknologisk information utomlands. De hade också bistått med säkerhetstjänst och i viss mån även försett rysk industri med ledare.

Ryssland hade dock ett antal problem att hantera vad gällde att tillgodogöra sig den inhämtade informationen. Vid sidan av fördelarna med underrättelse- och säkerhetstjänsternas stöd till rysk forskning och industri, fanns även ett antal uppenbara risker. Även om stöd från de hemliga tjänsterna kan framstå som en lovande genväg till modernisering, kan detta långsiktigt visa sig vara en återvändsgränd.

I denna rapport analyseras de ryska underrättelse- och säkerhetstjänsternas stöd till inhemsk forskning och industri utifrån officiella ryska dokument och publikationer av forskare, före detta underrättelseofficerare och utländska underrättelsetjänster. Såväl möjligheter som hinder och risker med stöd från hemliga tjänster i dagens ryska kontext behandlas i rapporten.

Nyckelord: Ryssland, underrättelsetjänster, säkerhetstjänster, vetenskap, industri, teknologi, forskning och utveckling (FoU), innovation, modernisering.

Acknowledgements

Carolina Vendil Pallin, head of the FOI Russia Research Project insisted that this study should be developed into a report rather than appear in an appendix in another publication. Her encouragement and expertise on Russia and its intelligence services have contributed greatly.

Other colleagues at FOI have also made contributions that have enriched this report. Roger Roffey has been most helpful in sharing his expertise on Russian biotechnology and the Soviet biological weapons programme. Roland Heickerö has guided me to sources in the world of cyber espionage and Fredrik Lindvall has shared his knowledge of intelligence methods.

Colleagues outside FOI have also generously shared their deep understanding of intelligence issues. I am grateful for the helpful advice of Jan Leijonhielm and Lars Nicander at the Swedish National Defence College and Wilhelm Unge at the Swedish Security Service. Others have preferred not to be mentioned by name, but that does not diminish my gratitude to them.

Finally, Eve Johansson's skills as language editor significantly improved the text. I am deeply grateful for the many improvements suggested to this report; any remaining errors should be attributed to me alone.

Fredrik Westerlund
April 2010

Table of Contents

Acronyms and abbreviations	1
Introduction	2
Historical precedents: Soviet S&T intelligence	5
Russian scientific and technological intelligence	11
Intelligence support to science: opportunities and obstacles	15
S&T intelligence gathering.....	15
Providing security, business intelligence and management	20
Support from intelligence services: the risks for science and industry	24
Industrial espionage – a promising short cut or a dead end?	28
References	30
About the author	34
Selected FOI reports on Russia	35

Acronyms and abbreviations

BfV	Bundesamt für Verfassungsschutz (German national security service)
FAPSI	Federalnoe agenstvo pravitelstvennoi sviazi i informatsii pri Prezidente RF (Federal Agency for the Protection of Government Communications, 1991–2003)
FSB	Federalnaia Sluzhba Bezopasnosti Rossiiskoi Federatsii (Federal Security Service of the Russian Federation, 1995–)
FSK	Federalnaia Sluzhba Kontrrazvedki (Federal Counterintelligence Service, 1991–1995)
GKNT	Gosudarstvennyi Komitet Soveta Ministrov SSSR po Nauke i Tekhnike (State Committee for Science and Technology)
GRU	Glavnoe Razvedyvatelnoe Upravlenie (Main Intelligence Directorate, 1918–)
KGB	Komitet Gosudarstvennoi Bezopasnosti (Committee for State Security, 1954–1991)
NKVD	Narodnyi Komissariat Vnutrennikh Del (People’s Commissariat for Internal Affairs)
OGPU	Obedinennoe Gosudarstvennoe Politicheskoe Upravlenie (Joint (All-Union) State Political Directorate, 1923–1934)
R&D	research and development
RF	Russian Federation
S&T	science and technology
SVR	Sluzhba Vneshnei Razvedki (Foreign Intelligence Service, 1991–)
VPK	Voенно-Promyshlennaia Kommissiia (Military-Industrial Commission)

Introduction

The Russian Federation (RF) aspires to be a great power, not only through its possession of nuclear arms, but also by being among the largest economies in the world. Recognition as a leading scientific nation also supports the claim to great power status, but the contribution made by the national science base to Russia's economic development is even more important. This is perhaps the main explanation as to why innovation has been a recurring theme in the speeches of Dmitrii Medvedev since he was elected president in 2008. The need for innovation also figured in the RF National Security Strategy from 2009.¹

The Russian president has taken a keen interest in boosting science and industry, by identifying five high-technology areas: energy, information technology (IT), telecommunications, biomedicine and nuclear technology. Nanotechnology has also been singled out as an important area and in March 2010 plans were announced for scientific-technological centres for the development and commercialisation of contemporary technologies inspired by the success of Silicon Valley.²

There are many ways to boost national science and technology (S&T), as well as industry, and each state tends to use a number of options in conjunction with each other. Increased spending on domestic research and development (R&D) is one way to stimulate S&T; intensifying and deepening international cooperation is another. Furthermore, the government can work with a multitude of instruments to create an environment conducive to innovation and research, such as making it economically rewarding through legislation that protects intellectual

property, through eliminating corruption and bureaucracy that stifles entrepreneurship, and through supporting creative research milieus.

An additional way is to acquire foreign know-how and technology through espionage. This path is particularly tempting for countries with limited possibilities as regards the two first options or for those that believe they are too far behind the competition.

In 2010, there was little doubt that the intelligence services of the Russian Federation were active in S&T intelligence collection directed at foreign states. This conclusion is supported by official Russian documents and historical precedents as well as assessments by scholars, former Russian intelligence officers and foreign intelligence services. The impact of the intelligence gathered on the performance of Russian R&D and industry is, however, much more difficult to assess. Fully exploiting S&T intelligence demands significant domestic scientific and industrial resources.

It is furthermore not always obvious that intelligence support for domestic science and industry is easily compatible with the other avenues for stimulating research and development. In the following, the Russian intelligence services' support to domestic science and industry and its potential effects will be explored. From historical precedents, official documents and expert opinions, the current state of Russian S&T intelligence is assessed. Possible areas of support to Russian science and industry, such as gathering intelligence, and providing security and management, are discussed below as well as the obstacles to and risks associated with intelligence support. The impact of the Russian intelligence services in other sectors of society falls outside the scope of this report, as does S&T intelligence gathering for the benefit of the intelligence services themselves.³

¹ Russian Federation (2009) 'Strategiia Natsionalnoi Besopasnosti Rossiiskoi Federatsii do 2020 goda [National Security Strategy of the Russian Federation up to 2020]', Russian Security Council, 12 May 2009 (by Presidential Decree No. 537), on the Internet: <http://www.scrf.gov.ru/documents/99.html>, paragraphs 24 and 66–68.

² President of Russia (2010b) 'Vstrecha s pobediteliami shkolnykh i studenticheskikh olimpiad [Meeting with participants in the pupil and student olympiad]', on the Internet: <http://www.kremlin.ru/news/7139> (retrieved 24 March 2010).

³ Intelligence services usually gather scientific and technical information in order to develop methods and technology for their own purposes. It has been estimated that in 1980, 28 per cent of the intelligence gathered by the S&T arm of the KGB (the all-union Soviet civilian intelligence service) went to the KGB itself as well as other government agencies; see Andrew and Mitrokhin (1999) *The Mitrokhin Archive* (London, Penguin Press), p. 285.

This report is based on open information, which always presents methodological problems when studying secret organisations. Even though the number of official statements and news items concerning Russian intelligence services was at a historical high at the turn of the 21st century, the information available on the current organisations and operations was scant. However, much more historical data have been available to researchers thanks to increased access to archives during some periods after the fall of the Soviet Union. Furthermore, the end of the Cold War has also allowed for a plethora of accounts to be provided by intelligence operators on both sides of the Iron Curtain.

Information retrieved from archives as well as statements by current and former intelligence agents must be treated with caution when used for assessing the intentions and capacity of Russian intelligence services. Some tentative conclusions can nevertheless be made concerning Russian intelligence support to domestic science and industry. These are presented in the following, with the caveat that additional information becoming available in the future may prove the conclusions to be inaccurate.

Historical precedents: Soviet S&T intelligence

During the Soviet era, the intelligence services continuously supported large-scale scientific efforts. From the implementation of the first five-year plans and the massive industrial effort of the Second World War, through the development of nuclear and biological weapons and up to the arms race in the 1980s, Russian science and industry was boosted by Russian intelligence operations abroad. This was no aberration in the Soviet system, because the intelligence services formed an inseparable part of it. That they would contribute to industrial development was natural, given that the Soviet Union 'did not *have* an MIC [military-industrial complex], rather it *was* one', as Stephen J. Blank has pointedly remarked.⁴

The reliance on foreign know-how was one of the main characteristics of Soviet R&D throughout the Soviet Union's existence.⁵ The USSR created the world's largest legal and illegal S&T information-gathering apparatus. The system worked as a supplement to, but also a substitute for, domestic R&D.⁶ During the Soviet era, intelligence support to science and industry was the norm, not the exception, as the following examples indicate.

The realisation of the Soviet Union's first five-year plans in the late 1920s and in the 1930s was highly dependent on foreign know-how and machinery, notably American. Much was readily available through trade agreements and professional exchange programmes, but some was acquired by intelligence operations in the USA. Both the civilian

⁴ Blank (2007) *Rosoboroneksport: Arms Sales and the Structure of Russian Defence Industry*, (Carlisle, PA, Strategic Studies Institute, U.S. Army War College, January 2007), p. 3.

⁵ For a brief description of Soviet S&T intelligence gathering (in Swedish), see Leijonhielm et al. (2002) *Den ryska militärtekniska resursbasen: Rysk forskning, kritiska teknologier och vapensystem [Russian Military-Technological Capacity: Russian R&D, Critical Technologies and Weapon Systems]* (Stockholm, Swedish Defence Research Agency), pp. 43–7. The report contains a short summary in English on pp. 12–13.

⁶ Almquist (1990) *Red Forge – Soviet Military Industry Since 1965* (New York, Columbia University Press), pp. 79 and 111.

intelligence service, the OGPU⁷ (which became part of the NKVD⁸ in 1934), and its military counterpart, the GRU,⁹ performed industrial espionage in the USA. Intelligence was gathered by officials within the Soviet Union's purchasing agency, Amtorg Trading Corporation, the International Communist movement (or Comintern) and embassies and consulates, as well as by illegal residents.¹⁰

In order to support the war effort, the NKVD reorganised in April 1941 and created a new department for scientific and technical espionage separate from political intelligence collection, signalling an increase in the priority being given to scientific intelligence.¹¹ The Soviet-US Lend-Lease Agreement opened up opportunities for intelligence gathering concerning science and technology, and the Soviet intelligence services took advantage of this to gain information about American cutting-edge industrial processes and technology.¹² Steven T. Usdin notes that the spy ring headed by Julius Rosenberg 'supplied the USSR with blueprints for every major U.S. military technology developed during World War II'.¹³ Two members of the spy ring continued to contribute to Soviet scientific

⁷ The Joint (All-Union) State Political Directorate (Obedinennoe Gosudarstvennoe Politicheskoe Upravlenie, OGPU) was the name of the Soviet secret police from 1923 to 1934, when it was returned to the NKVD (see next footnote).

⁸ The Russian Soviet Federative Socialist Republic (RSFSR) People's Commissariat for Internal Affairs (Narodnyi Komissariat Vnutrennikh Del, NKVD) included the RSFSR secret police, the GPU (Gosudarstvennoe Politicheskoe Upravlenie) from its creation in February 1922 to November 1923, when the GPU was incorporated in the all-union secret service, the OGPU. In July 1934, the RSFSR NKVD was transformed into an all-union NKVD and the OGPU was incorporated under the acronym GUGB (Glavnoe Upravlenie Gosudarstvennoi Bezopasnosti, the Main Directorate for State Security). In April 1943, the secret police, having been renamed the NKGB (Narodnyi Komissariat Gosudarstvennoi Bezopasnosti, People's Commissariat for State Security) in 1941, was separated from the NKVD.

⁹ The Main Intelligence Directorate (Glavnoe Razvedyvatelnoe Upravlenie, GRU) of the General Staff of the Armed Forces was created on 21 October 1918.

¹⁰ Sibley (2004) *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* (Lawrence, Kansas, University Press of Kansas), pp. 16–7, 38 and 51; p. 25 and 31.

¹¹ Andrew and Mitrokhin, *The Mitrokhin Archive*, p. 141.

¹² Sibley, *Red Spies in America*, p. 93.

¹³ Usdin (2009) 'The Rosenberg Ring Revealed: Industrial-Scale Conventional and Nuclear Espionage', *Journal of Cold War Studies*, Vol. 11, No. 3, Summer 2009, p. 122. For a summary of major technologies transferred through the Rosenberg spy ring, see Table 2 in that article, *Inferred Non-Nuclear Technology Transfer*, pp. 119–20.

and technical development for several years after they were exposed, after having fled to the USSR.¹⁴

The Soviet intelligence services also played an important role for another huge Soviet scientific undertaking – the nuclear weapons programme. In 1941 both the NKVD and the GRU received intelligence on Allied scientific advances regarding the construction of an atomic bomb. By the beginning of 1945, the Soviet intelligence services had a clear picture of the US as well as the joint British–Canadian nuclear weapons projects.¹⁵

The scientific and technical intelligence gathered was shared with the scientific director of the Soviet atomic bomb programme, Igor Kurchatov, and had an undisputed impact. Early in the process, intelligence influenced the scientific paths chosen towards fulfilment of the project and it continued to have an immense impact in the later stages as well.¹⁶ The former Soviet intelligence officer Alexander Feliksov has noted that thanks to the spy Klaus Fuchs, the first three Soviet bombs were copies of US models.¹⁷

Furthermore, information provided by the intelligence services probably gave the impetus to the development of a thermonuclear weapon, even though the first hydrogen bomb was of Soviet design.¹⁸ The extensive intelligence information was kept within a very narrow circle of leading scientists and managers, and was considered by Kurchatov to be of great importance. He also began requesting additional information and thus took an active part in the intelligence process by contributing to the formulation of intelligence requirements.¹⁹

The Soviet intelligence services did not merely contribute crucial information on how to build an atomic bomb; NKVD director Lavrentii Beria was put personally in charge of the nuclear weapons programme.

¹⁴ Ibid., p. 139.

¹⁵ Holloway (1994) *Stalin and the Bomb* (New Haven, Yale University Press), pp. 82–4; 105.

¹⁶ Ibid., pp. 90–95, with reference to 'U istokov sovetskogo atomnogo proekta: Rol Razvedki 1941–1946 gg.' *Voprosy istorii estestvoznaniia i tekhniki*, 1992, no. 3, pp. 107–8, 106–108, 173 and 222.

¹⁷ Feliksov, Aleksander (2001) *The Man behind the Rosenbergs* (New York, Enigma Books), p. 201, cited in Sibley, *Red Spies in America*, p. 168.

¹⁸ Holloway, *Stalin and the Bomb*, p. 296; p. 303.

¹⁹ Ibid., pp. 96 and 102–4.

Beria got this assignment not only because he was a talented organiser but also due to his position as head of the most feared and efficient state organisation.²⁰ As director of the NKVD, Beria also commanded the Gulag²¹ prison system, which provided the workforce for the necessary mining and construction tasks within the nuclear bomb programme. Beria also brought in some of the scientists involved in the project from the Gulag prison camps. Kurchatov served as the main scientific advisor to Beria and, as David Holloway has pointed out, in this way 'scientific advice and political authority were effectively combined.'²²

Another scientific undertaking heavily influenced by the Soviet intelligence services was the extensive biological weapons (B-weapons) programme. In the very first years of the Soviet Union's existence, Lenin created a secret laboratory to cater for the intelligence services' needs for undetectable poisons.²³ In the late 1920s, the possibilities of producing B-weapons in the Soviet Union were explored²⁴ and later a B-weapons programme was initiated. The programme expanded over the years and in the late 1970s a new department was created within Directorate S of the First Main Directorate (Foreign Intelligence) of the KGB²⁵ to cater for the intelligence needs related to biological warfare.²⁶

²⁰ Ibid., p. 134 and 221.

²¹ The Gulag (Glavnoe upravlenie lagerei, Main Camp Administration) has come to signify not only the organisation for administration of the concentration camps, but the entire Soviet system of slave labour. The system was controlled by the domestic intelligence service, and supplied the Soviet state with both unskilled labourers and top scientists. For a thorough account of the subject, see Appelbaum (2003) *Gulag: A History* (London, Penguin Group). The use of scientists is exemplified on pp. 118–9.

²² Holloway, *Stalin and the Bomb*, p. 141.

²³ Volodarsky (2009) *The KGB's Poison Factory: From Lenin to Litvinenko* (Barnsley, S. Yorkshire, Frontline Books), p. 32–3.

²⁴ According to Yakov Fishman, the head of the Military-Chemical Directorate of the Worker-Peasant Red Army (RKKA), Soviet interest in B-weapons dates back to at least 1928 when he prepared a report on biological warfare: see Fishman, Ya., 'Rabota Bakteriologicheskoi Laboratorii VOKHIMU' [Work of the Bacteriological Laboratory of the Military-Chemical Directorate], Russian State Military Archive, fond 33987, op. 1, d. 657, 1.143-144, 10 February 1928, quoted in Stoecker (1998) *Forging Stalin's Army: Marshal Tukhachevsky and the Politics of Military Innovation* (Boulder, Colorado, Westview Press), ref. 69, p. 109.

²⁵ The Committee for State Security (Komitet Gosudarstvennoi Bezopasnosti, KGB) was the name of the all-union Soviet civilian intelligence service from March 1954 to the fall of the Soviet Union in the autumn of 1991.

²⁶ Kouzminov (2005) *Biological Espionage: Special Operations of the Soviet and Russian Foreign Intelligence Services in the West* (London, Greenhill Books), p. 32.

Directorate S handled all the illegal KGB agents abroad, and the new department, Department 12, was to focus on gathering intelligence on biological weapons abroad as well as using them. The information gathered abroad was regularly forwarded to the Directorate for Scientific and Technological Intelligence (Directorate T) and to secret laboratories connected to Department 12, but also to other research institutions through KGB departments at institutes or officers working under cover and posing as ordinary research scientists.²⁷

Finally, the US-Soviet arms race in the 1980s ensured that the Soviet intelligence services maintained a strong interest in scientific and technical information with military applications. Research on and the development of new weapon systems in the Soviet Union were facilitated by intelligence gathering in the USA, not least concerning naval and aircraft design.²⁸

Even at the height of the *glasnost* (openness) era, Soviet spies remained highly active in intelligence gathering. The targets of the industrial espionage effort included for instance semiconductors, computer-aided design systems, fibre optics and nuclear energy.²⁹ According to Christopher Andrew and Vasili Mitrokhin, Soviet leader Mikhail Gorbachev regarded industrial espionage as an important part of the economic *perestroika* (restructuring) of the country.³⁰

The extensive Soviet S&T information-gathering effort involved not only the foreign intelligence services but also other parts of the state bureaucracy. Apart from the KGB and the GRU, foreign know-how was collected by the State Committee for Science and Technology (Gosudarstvennyi Komitet Soveta Ministrov SSSR po Nauke i Tekhnike, GKNT), the State Committee for Foreign Economic Relations (Gosudarstvennyi Komitet po Vneshnim Ekonomicheskim Sviaziam, GKES) and a secret department of the Russian Academy of Sciences. The largest and most important intelligence-collecting organisation was the

²⁷ Ibid., p. 32; p. 76; pp. 34–8.

²⁸ Sibley, *Red Spies in America*, p. 232.

²⁹ Ibid., pp. 221–2 and 233.

³⁰ Andrew and Mitrokhin, *The Mitrokhin Archive*, p. 287.

KGB and its Directorate T,³¹ but it is worth noting the intermediate role played by the Russian Academy of Sciences, connecting the intelligence services with foreign scientists and linking Soviet civil with military R&D.

The GKNT not only gathered foreign S&T information; it also coordinated the entire civilian industrial research activity and put together the requirements for the collection of intelligence concerning civilian R&D. Its counterpart where military R&D was concerned was the powerful Military-Industrial Commission (Voenno-Promyshlennaia Kommissiia, VPK). These two organisations managed the prioritisation, selection, approval and follow-up of Soviet civil and military R&D projects, and thus also controlled foreign S&T intelligence collection.³²

In conclusion, however, it is worth noting that the Soviet strategy of extensive intelligence support to domestic science and industry did not give the Soviet Union a technological and economic advantage. From the early 1970s, the gap between Soviet and Western industrial capacity grew visibly and in the late 1980s Soviet industry was competitive only in a few, mostly military, branches.

Russian scientific and technological intelligence

In 2010, Russia made no secret of its ambitions to gather S&T intelligence for the benefit of its interests. Since 1995, the Russian intelligence services have been obliged by federal law 'to assist the country's economic development and its scientific and technical progress and to ensure the military-technical security of the Russian Federation'.³³ These words were echoed in the officially declared goals and tasks for the SVR,³⁴ the Russian Foreign Intelligence Service.³⁵ Foreign S&T intelligence operations have mainly been the responsibility of the SVR and the military intelligence service, the GRU.³⁶ By 2010 both organisations had for many years comprised separate directorates for scientific and technological intelligence.³⁷

After the end of the Cold War, S&T intelligence became all the more important to the Russian intelligence services. According to a statement made in 1992 by the Russian defector Stanislav Levchenko, high-tech industrial and economic intelligence had become the main priority for the new Russian intelligence service.³⁸ In 2004, the American scholar

³¹ Andrew and Gordievsky (1990) *KGB – The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (London, Hodder & Stoughton), pp. 521–2.

³² Barron (1974) *KGB – The Secret Work of Soviet Secret Agents* (New York, Reader's Digest Association), pp. 141–2.

³³ Russian Federation (1995) *Federalnyi zakon 'O vneshnei razvedke'* [Federal Law 'On Foreign Intelligence'] No. 5-F3, Article 5.

³⁴ The Foreign (literally External) Intelligence Service (Sluzhba Vneshnei Razvedki, SVR) is the successor to the KGB First Main Directorate (Foreign Intelligence).

³⁵ See for instance the SVR website: http://www.svr.gov.ru/svr_today/ceci.htm, as of March 2010.

³⁶ The GRU is under the control of the Russian General Staff of the Armed Forces. One of the officially recognised functions of the latter has for many years been to 'carry out intelligence activity in the interest of the defence and security of the Russian Federation': see RF Ministry of Defence, 'Polozhenie "O Generalnom shtabe VS RF" [Decree "On the General Staff of the Armed Forces of the Russian Federation"]', on the Internet: <http://www.mil.ru/847/852/1153/1339/1826/index.shtml> (retrieved 20 March 2010), Chapter III, paragraph 17.

³⁷ In 2001, the GRU was reported as having a (Ninth) Directorate for Military Technology: see Lekarev (2001) 'Dva vida rossiiskoi razvedki unifitsiruiutsia [Two types of Russian intelligence become unified]', *Nezavimoe Voennoe Obozrenie*, on the Internet: http://nvo.ng.ru/spforces/2001-08-31/7_unification.html (retrieved 10 March 2010). The SVR official organisation chart in 2010 showed a Directorate for Scientific and Technological Intelligence (NTR) directly subordinated to the Deputy SVR Director for Science: see the SVR website: http://www.svr.gov.ru/svr_today/struk_sh.htm, as of March 2010. This would be the successor to

Directorate T (Science and Technology) of the KGB First Main Directorate (Foreign Intelligence).

³⁸ Sibley, *Red Spies in America*, p. 233.

Katherine Sibley argued that Russian collection of scientific intelligence would probably continue for years to come:

[W]artime military-industrial espionage practises established a template for Soviet and later Russian intelligence gathering that remains in use to this day; as long as U.S. technology maintains its preeminent global position, such espionage will likely continue [...].³⁹

This would apply not least to the expanding field of biotechnology. The SVR inherited an extensive biotechnology intelligence-gathering organisation from its Soviet predecessor. In 2005, the former Department 12 intelligence officer Alexander Kouzminov expressed doubts that such a power had been abandoned because of détente and democratisation.⁴⁰

The assessments of scholars and former Russian intelligence officers are supported by statements from foreign counter-intelligence services. In the 2010 annual threat assessment by Dennis C. Blair, Director of US National Intelligence, the Russian Federation was singled out as a significant intelligence threat. 'Russia continues to strengthen its intelligence capabilities and directs them against US interests worldwide. Moscow's intelligence effort includes espionage, technology acquisition and covert action efforts', Blair reported to the US Senate.⁴¹

The German national security service, the Bundesamt für Verfassungsschutz (BfV) in its 2008 annual report also acknowledged the Russian Federation as one of the main intelligence actors in Germany, in particular in the areas of science and technology.⁴² In 2008, the emphasis where Russian S&T intelligence gathering was concerned was in computer, telecommunications and security technology, as well as in products in the fields of measurements and aeronautics. The BfV stated

that Russia also showed interest in military technology products and civil defence technology with military applications.⁴³

In 2007, the head of the British Security Service (also known as MI5), Jonathan Evans, complained that Russian and Chinese intelligence activity in Great Britain was forcing the Security Service to divert resources from the fight against terrorism. According to Evans, the scope of the Russian intelligence gathering was equal to the Soviet effort during the Cold War. He also stated that Russian intelligence services were particularly interested in British science and technology.⁴⁴

It is also worth noting that in March 2010 a Russian parliamentarian spoke up for S&T intelligence as a preferable alternative to buying foreign technology. In a hearing in the State Duma on the proposed acquisition of French-designed Mistral amphibious assault ships, the cosmonaut and Communist Party Duma Deputy Svetlana Savitskaia is reported to have urged the Russian Government to task the military-technological intelligence service to gather the necessary know-how, rather than to buy technology from abroad.⁴⁵ The statement indicates a popular conception of foreign intelligence gathering as a viable alternative, but the government's plans for purchasing Mistral ships suggest that the Kremlin did not share that view in this particular case.

Even though the intent was clear and the organisation for intelligence gathering was in place in the early 21st century, there were some doubts regarding the efficiency of the post-Soviet intelligence services. The former KGB officer Alexander Kouzminov has stated that one of the main reasons for his resignation in 1992 was that the intelligence operations in his department were to an increasing extent carried out in the personal interest of his bosses.⁴⁶ The pursuit of personal gain, for which opportunities were abundant to enterprising foreign intelligence officers

³⁹ Ibid., p. 11.

⁴⁰ Kouzminov, *Biological Espionage*, p. 109.

⁴¹ US Director of National Intelligence (2010) *Annual Threat Assessment of the US Intelligence Community for the Senate select Committee on Intelligence* (Washington, D.C., Office of the Director of National Intelligence, 2 February 2010), p. 43.

⁴² Bundesamt für Verfassungsschutz (2009) *Verfassungsschutzbericht 2008* (Berlin, Bundesministerium des Innern), p. 308 and 335.

⁴³ Ibid., pp. 312–3.

⁴⁴ Brogan (2007) 'Soaring Number of Russian and Chinese Spies Diverting MI5 Attention from Terror Fight', *Daily Mail*, on the Internet: <http://www.dailymail.co.uk/news/article-491830/Soaring-number-Russian-Chinese-spies-diverting-MI5-attention-terror-fight.html> (retrieved 27 January 2009).

⁴⁵ *Nezavisimaia Gazeta* (2010) 'V golubom vertolete [In the blue helicopter]', on the Internet: http://www.ng.ru/titus/2010-03-11/1_filantropia.html (retrieved 17 March 2010).

⁴⁶ Kouzminov, *Biological Espionage*, pp. 144–5.

in the early 1990s, were damaging to the efficiency of the intelligence organisation.

It is nevertheless probable that Russian national scientific or industrial efforts in 2010 and beyond, for instance in nanotechnology or biotechnology, will be actively supported by the Russian intelligence services, not least since the political leadership may be inclined to encourage the foreign intelligence services to support domestic R&D; and several prominent politicians, including Prime Minister Vladimir Putin, have personal experience of intelligence service work. In 2010 it was not so much a question of whether Russia would gather intelligence in support of its industry as of how effective that intelligence gathering would be.

Intelligence support to science: opportunities and obstacles

Intelligence services can support national science and industry in more than one way. They can provide access to foreign S&T or commercial secrets and help protect domestic know-how from being stolen by other states and foreign companies. Intelligence agencies can also provide managerial and bureaucratic support to foster science and innovation. However, alongside the opportunities offered by involving intelligence services and methods in scientific and industrial undertakings, there are obstacles to be overcome.

S&T intelligence gathering

The Russian intelligence services have a proven capacity to collect and pass on information on foreign know-how, research and technologies to Russian science and industry. Russia's multiple intelligence agencies have long been able to operate under the cover of Russian Federation diplomatic missions abroad as well as approach foreign researchers and entrepreneurs in Russia. The intelligence services also have a long tradition of posting illegal agents in their target countries, often by first establishing a career in one or several third countries, such as China, Sweden or Canada.⁴⁷ This allows Russian agents to use academic research institutions or commercial companies as platforms for espionage activity.⁴⁸

It should however be noted that the successes of human intelligence gathering in the Soviet era may be difficult to repeat, as one of the main motivators for foreign spies during that time – an attractive ideology – no longer exists. Loyalty to a common cause is no longer the main driver, as it was, for example, with Julius Rosenberg and his comrades.⁴⁹ Monetary

⁴⁷ C.f. *ibid.*, pp. 79–80, 93–4 and 102–3. Concerning a recent case of an SVR illegal in Canada, see Lefebvre (2007) 'Russian Intelligence Activities in Canada: The Latest Case of an "Illegal"', *Journal of Slavic Military Studies*, Vol. 20, pp. 549–58.

⁴⁸ Kouzminov, *Biological Espionage*, pp. 136–9.

⁴⁹ Usdin, 'The Rosenberg Ring Revealed', p. 94.

rewards and extortion can still inspire foreigners to divulge information, but are not as reliable as motivators.

Furthermore, during the Soviet era a large part of the S&T intelligence was obtained through the intelligence services of the Warsaw Pact countries. In 1980, more than half of the intelligence obtained by the KGB Directorate T⁵⁰ came from allied services, according to Christopher Andrew and Vasili Mitrokhin.⁵¹ The opportunities to obtain intelligence through allied intelligence services have been considerably reduced since the fall of the Soviet Union.

An alternative way to acquire scientific and industrial intelligence is through cyber espionage. This is a rapidly growing field of intelligence: in 2008 more than 1 trillion US\$-worth of data was reportedly lost to cyber espionage in the USA alone.⁵² Together with China, Russia has been named by US sources as acting aggressively in this respect.⁵³ In 2009, the Russian Federation was one of five countries assessed to be developing advanced offensive cyber capabilities.⁵⁴ A FOI report concluded in 2010 that the Russian intelligence services possessed the necessary resources to conduct cyber operations.⁵⁵ Apart from cyber espionage, scientific and technological intelligence can be obtained by signals intelligence, another area where the Russian intelligence services have a solid Soviet foundation to build upon.

However, even if Russia possesses methods as well as technical and human resources for extensive collection of S&T intelligence, that does not automatically imply dividends for domestic science and industry. It may prove difficult to transfer foreign technology and know-how to Russian research institutions and industrial enterprises, for several reasons.

⁵⁰ The S&T branch of the KGB First Main Directorate (Foreign Intelligence).

⁵¹ Andrew and Mitrokhin, *The Mitrokhin Archive*, p. 285.

⁵² Ackerman (2009) 'Threats Imperil the Entire U.S. Infostructure', *SIGNAL Magazine, AFCEA International Journal*, July 2009.

⁵³ Heickerö (2010) *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm, Swedish Defence Research Agency (FOI), March 2010), p. 35.

⁵⁴ McAfee (2009) *Virtual Criminology Report 2009*, McAfee, Inc., p. 13.

⁵⁵ Heickerö, *Emerging Cyber Threats*, p. 34. See also pp. 27–31.

For one, a successful transfer of technology is dependent on the capacity of the recipients to make use of the information they are supplied with. Christopher Andrew and Vasili Mitrokhin argue that the Soviet military industry greatly benefited from foreign intelligence operations, but the dividends were small in civilian production despite intensive intelligence support:

The real economic benefit of Western scientific and technological secrets, through put by Directorate T at billions of dollars, was, however, severely limited by the structural failings of the command economy. The ideological blinkers of the Soviet system were matched by its economic rigidity and resistance to innovation by comparison with the market economies of the West. Hence the great economic paradox of the 1980s: that despite possessing large numbers of well-qualified scientists and engineers and a huge volume of S&T, Soviet technology fell steadily further behind its Western rivals.⁵⁶

An example of less successful transfer of civilian S&T intelligence is the Soviet supersonic Tu-144 airliner. The aircraft, which first appeared in the West at the 1973 Paris Air Show, was dubbed 'Concordski' due to its striking similarities with the Anglo-French Concorde. According to Andrew and Mitrokhin, the KGB had acquired close to 100,000 pages of detailed technical specifications on several new aircraft, including Concorde, through a British aeronautical engineer recruited in 1967.⁵⁷ However, despite the similarities in design, the technology applied in the development of the Tu-144 was to a great extent of Soviet origin. The Paris Air Show visit ended in disaster when the Tu-144 crashed, and even though several aircraft were produced, the Tu-144 was taken out of service after only three years.

Intelligence can compensate for inadequate domestic know-how, but only to a certain extent. In order to emulate foreign S&T, the scientists and engineers need to have a sufficient understanding of the underlying principles. This is necessary if they are to be able not only to reproduce the results that have been gleaned, but also to spot errors in the information provided by the intelligence services. Inaccuracies can occur due to errors made by the foreign scientists and engineers in the first

⁵⁶ Andrew and Mitrokhin, *The Mitrokhin Archive*, p. 724.

⁵⁷ *Ibid.*, p. 549. It has furthermore been alleged that French intelligence fed the Soviet spies false design information after discovering that the Concorde programme had been penetrated by Soviet foreign intelligence; see e.g. *The History of Tupolev TU-144*, on the Internet: <http://tu144.tripod.com/history.html> (retrieved 19 April 2010).

place or originate from mistakes made in the intelligence-gathering process. False information can also have been inserted by foreign counter-intelligence services as part of an intelligence war, so that every piece of information needs to be carefully evaluated. To fully exploit foreign S&T, national R&D resources also need to be sufficiently developed to allow successful adaptation of the information that has been gathered and evaluated to domestic societal needs.

Twenty years after the fall of the Soviet Union, the Russian Federation was still benefiting from the legacy of efficient intelligence services, but at the same time it was struggling with the other inherited aspects of the Soviet system, such as the lack of an innovation culture within industry. Another Soviet legacy that continued to affect Russian industry negatively in the 21st century was its out-of-date machinery and production lines. Even though Russian science has been internationally competitive in many areas in the post-Soviet era, large parts of domestic industry have found it difficult to convert scientific advances into competitive mass-produced products.

The intelligence services could most probably assist by supplying information on modern production techniques and samples of high-tech machinery. However, the contribution of Russian intelligence would only be of marginal value, with the odd exception, unless it was accompanied with major investment in a large-scale overhaul and modernisation of Russian industry.

Another obstacle to the transfer of foreign S&T intelligence to scientists and engineers for the benefit of national industry is the need for security in intelligence operations. The most valuable assets of an intelligence agency are its sources and methods. A profitable source or method usually has been developed over a long period of time and at considerable cost, but the investment may quickly come to nothing if a source or a method is compromised.

Secrecy and security are therefore necessary as protection, but at the same time this constitutes a hurdle to the successful transfer of know-how and technology to open research organisations and commercial industry. Even in the closed Soviet society, the intelligence services were often

cautious when passing on information,⁵⁸ and the need for discretion is even greater in the much less rigidly controlled Russian society.

Finally, another vital aspect of intelligence work could prove problematic: defining intelligence requirements. This is partly connected to the aspect of secrecy just mentioned. In order to fine-tune intelligence requirements and optimise the collection effort, you need detailed knowledge not only concerning the state of your own country's science, but also about available intelligence methods and sources.

Otherwise the scientist may ask for information the intelligence service cannot access, and the latter may spend time and resources on obtaining information that the scientists and engineers have no use for. Close collaboration between scientists and intelligence operators enables efficient intelligence gathering by clearly defining the intelligence requirements. However, it risks compromising secrecy and security in intelligence operations.

Apart from the hurdle to efficient tasking raised by secrecy concerns, the different cultures in science and intelligence organisations may become an obstacle to successful cooperation and communication over defining intelligence requirements. Such hurdles can, however, be overcome, as the involvement of the leading scientist Igor Kurchatov in the intelligence gathering for the Soviet nuclear weapons programme, mentioned above, testifies.

According to Brian Freemantle, the S&T intelligence requirements of the Russian Foreign Intelligence Service in the years after the break-up of the Soviet Union were embodied in a 27-chapter book entitled *Coordinated Requests for Technological Information*.⁵⁹ That 'shopping list' was most probably a Soviet product, and keeping it up to date to the needs of Russian science and industry in the 21st century is no small undertaking for the Russian foreign intelligence services.

⁵⁸ For instance, the extensive intelligence information on the development of nuclear weapons was kept within a very narrow circle of leading scientists and managers: see Holloway, *Stalin and the Bomb*, pp. 96–7.

⁵⁹ Freemantle, Brian (1986) *The Steal: Counterfeiting and Industrial Espionage* (London, Michael Joseph), p. 9, cited in Sibley *Red Spies in America*, p. 233, ref. 54.

Providing security, business intelligence and management

Intelligence and security services can also promote domestic industry by providing commercial intelligence and protection from foreign espionage. The need to protect Russian science and technology as well as industry from foreign threats has been expressed in official documents, such as the national Information Security Doctrine presented in the year 2000.⁶⁰

The main external threats in the area of science and technology were identified as the efforts of other states to gain access to Russian S&T resources for their own benefit and to create a beneficial situation on the Russian market for their companies at the expense of Russian competitors. Other main external threats were the perceived aspirations of the developed countries to hinder the development of Russia's S&T potential as well as policies on the part of the West directed at further disrupting the former Soviet united scientific-technological infrastructure inherited by the members of the Commonwealth of Independent States (CIS).⁶¹

Safeguarding Russian science and technology from foreign intelligence services and corporations has been one of the tasks of the domestic security service, the FSB,⁶² since its creation in 1995.⁶³ The FSB draws on extensive experience with counter-intelligence operations from its Soviet predecessor.

⁶⁰ Russian Federation (2000a) 'Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii [Information Security Doctrine of the Russian Federation]', Russian Security Council, on the Internet: <http://www.scrf.gov.ru/documents/5.html> (retrieved 30 March 2010).

⁶¹ Ibid., paragraph 6.

⁶² The Federal Security Service of the Russian Federation (Federalnaia Sluzhba Bezopasnosti Rossiiskoi Federatsii, FSB).

⁶³ The FSB is the main successor of the KGB, and received its name after having been known as the Federal Counterintelligence Service (Federalnaia Sluzhba Kontrrazvedki, FSK) between 1991 and 1995. In 2003, the Border Troops and large parts of the disbanded signals intelligence agency FAPSI (Federalnoe agenstvo pravitelstvennoi svyazi i informatsii pri Prezidente RF, Federal Agency for the Protection of Government Communications) were incorporated in the FSB, making it the largest Russian intelligence service.

It is a legitimate national interest to stop foreigners from stealing Russian know-how, but there is always a cost to security as it hampers the flow of information. The security mindset with its emphasis on risk reduction is in many ways the opposite of a climate conducive to research and innovation, that is, focusing on opportunities and encouraging risk-taking. Too much security thinking becomes an obstacle to science. There is also the problem of knowing which objects to protect – the institutions and companies that are most vulnerable, those that are most exposed or those that are most important to national development

Supplying commercial secrets to domestic enterprises in order to promote national industry is another tested form of intelligence service support. It could consist of traditional business intelligence, allowing bench-marking or ensuring the best bid: confidential information on a competitor's products, production processes and organisation as well as on competing bids can be highly valuable to a company and give a competitive edge. Intelligence services could also assist in a more indirect way by monitoring foreign competitors in order to reveal foul play in their business methods. Apart from human collection, cyber espionage and signals intelligence stand out as effective methods for providing commercial intelligence.

However, providing business intelligence support is not simple. The risk of compromising sources or methods is, of course, a hurdle to overcome in this aspect too. Another challenge where state-sponsored business intelligence is concerned is how to decide which companies to assist. In an age of ever-increasing globalisation and expanding cross-border ownership and cooperation among commercial firms, it may be difficult to decide which companies are truly national as opposed to multinational or foreign. At the beginning of the 21st century, this was no serious challenge in Russia, due to the limited cross-border ownership in Russian industry.

Yet another way for intelligence services to contribute to the development of domestic science and industry is by providing able managers. High-level intelligence service officers may be singled out to coordinate national efforts within science, as well as other areas, because they are

perceived to possess the means for implementing grand plans. Just as NKVD head Lavrentii Beria was entrusted with the Soviet nuclear weapons programme, prominent former or serving intelligence officers may be deemed to have the necessary political and bureaucratic clout to promote contemporary scientific or industrial projects.

In 2010, several former intelligence service officers held top positions within Russian industry. Among the most prominent were three former KGB officers – Sergei Ivanov, Sergei Chemezov and Viktor Ivanov. Viktor Ivanov had been the chairman of the Board of Directors of the air defence system state corporation Almaz-Antei since 2002 and had held the corresponding position in the airline company Aeroflot since 2004.

Former Defence Minister Sergei Ivanov has many years of foreign intelligence experience and in 2007 was appointed as first deputy prime minister with responsibility for the defence industry, aerospace industry and nanotechnology. The same year he also became chairman of the Government Council for Nanotechnology. Since 2006, Sergei Ivanov had also served as the chairman of the board of the state-owned United Aircraft Construction Corporation (OAK).⁶⁴

Of the former KGB officers mentioned above, Sergei Chemezov had perhaps become the most influential in Russian industry. He had been appointed director general of the huge defence-industrial state corporation Russian Technologies (Rostekhnologiiia), after having headed Rosoboronekспорт for many years. Russian Technologies controls a large part of the Russian civilian and military industry through subsidiary companies, as well as all Russian arms exports. Chemezov also started his career as a foreign intelligence officer.

Another prominent person with an intelligence background is the alleged former GRU officer Igor Sechin. He has headed the Board of Directors of the oil giant Rosneft since 2004,⁶⁵ and has had the corresponding position in the state ship-building corporation OSK since it was created in 2007. Arguably, it seems likely that the professional background of these

former intelligence officers has been less of a decisive factor in their appointments than their close friendship to Vladimir Putin. However, such a friendship would perhaps not have developed without a shared professional background.⁶⁶ In this way, the Russian intelligence services can be said to have provided top managers for Russian industry in the early 21st century. A critical question here is whether the officers chosen have the managerial skills to foster innovation and a mindset conducive to expanding science and industry.

⁶⁴ OAK official website, http://www.uacrussia.ru/ru/corporation/guidance/soviet_directorov/, as of March 2010.

⁶⁵ Rosneft official website, <http://www.rosneft.com/about/board/>, as of March 2010.

⁶⁶ C.f. Gomart (2008) *Russian Civil-Military Relations: Putin's Legacy* (Washington, D.C., Carnegie Endowment for International Peace), p. 62.

Support from intelligence services: the risks for science and industry

Tempting as it may be to cut corners by relying on intelligence services to further national science and industry, there are several risks connected with industrial espionage. Reliance on intelligence may dull the edge of science and unintentionally restrict the access to foreign know-how. Even if it is possible to catch up with foreign competitors through espionage, it is hard to overtake them.

The often cited Lenin-inspired cliché of *dogmat' i peregnat'* (to catch up and overtake) the West is not feasible if scientific research is dependent on input from the intelligence services. Time spent on assessing information obtained by the intelligence services and assisting in the intelligence-gathering project is time not spent on developing one's own research. In some areas, like biotechnology, time is of prime importance as developments take place at an ever-increasing pace.

A Russian intelligence service effort to further Russian science and industry may, even if it is successful, be damaging in the long run. If the security services in other countries come to suspect that Russia is spying, the flow of knowledge in to Russia may suffer badly. Foreign companies and research institutions will be alerted to the risk of espionage and access to state-of-the-art science may be restricted for Russian researchers and engineers. Being associated with the intelligence services might not only ruin the international standing of an individual scientist or entrepreneur.⁶⁷ It will also taint the research organisation or company and limit opportunities for close cooperation with foreign actors.

Suspensions of spying could moreover hamper the inflow of knowledge across the research field for years to come. It may even be detrimental to

⁶⁷ For an example of a Russian scientist whose career in Sweden was set back by his involvement with a Russian intelligence officer, see the Swedish Security Service's account in the annual report for 2006 (in Swedish) of the arrest in February 2006 of a Russian scientist working at a Swedish university. Swedish Security Service (2007) 'Säkerhetspolisen 2006 [The Security Service 2006]', on the Internet: <http://www.sakerhetspolisen.se/download/18.7671d7bb110e3dcb1fd800019916/sakerhetspolisen2006.pdf> (retrieved 31 June 2009), p. 31.

Russian R&D in general, by undermining trustful cooperation with foreign actors in other areas as well. This would not be helpful to Russia's long-term security policy aims in the area of science and technology – 'to ensure the participation of Russian scientific and scientific-educational organisations in global technological and research projects'.⁶⁸

Furthermore, there is a risk of becoming your own enemy by mirror-imaging industrial espionage efforts. If you are prepared to use intelligence means and methods to lay your hands on scientific information, the suspicion that others might do the same easily becomes entrenched. Even without mirror-imaging, excessive vigilance towards foreign espionage due to zealous counter-espionage operations could do more harm than good by creating a climate of distrust.

In 2007, several instances of espionage charges brought against Russian academics were reported, and the then head of the FSB, Nikolai Patrushev, claimed that foreign espionage activity in Russia was increasing.⁶⁹ In December 2008, the head of the FSB directorate for the Saratov region expressed concern that foreign intelligence services were trying to obtain classified information as part of international scientific exchange programmes.⁷⁰

In January 2010, a director at one of the institutes of the Russian Academy of Sciences complained about the close attention the Russian security services were paying to Russian scientists and trumped-up charges of espionage.⁷¹ Close attention from the domestic security services to

⁶⁸ Russian Federation (2009) 'Strategiia Natsionalnoi Besopasnosti Rossiiskoi Federatsii [National Security Strategy]', paragraph 70.

⁶⁹ Racheva (2007) 'Space as Evidence', *Novaya Gazeta*, on the Internet: <http://en.novayagazeta.ru/data/2007/94/07.html> (retrieved, 20 April 2010); Rich (2007) 'Scientist Scientists? Risk Orosecution', *Times Higher Education*, on the Internet: <http://www.timeshighereducation.co.uk/story.asp?sectioncode=26&storycode=207675> (retrieved 25 March 2010).

⁷⁰ Interfax (2008) 'Foreigners Seeking High-tech Secrets in Saratov Region – Security Chief', Interfax News Agency (redistributed by BBC Monitoring Service). The FSB regional chief also singled out Russian nanotechnology and electronics research projects as being of particular interest to foreign special services.

⁷¹ Dziuba (2010) 'Sharashkina kontora [Sharashka's office]', *Novaya Gazeta*, on the Internet: <http://www.novayagazeta.ru/data/2010/003/00.html>. The title of the article is an expression borrowed from Russian slang and alludes to the Soviet secret R&D laboratories set up within the Gulag labour camp system, often referred to as *sharashkas*.

Russians who are in contact with foreigners can result in scientists declining to take part in international research projects or to receive funding from abroad, to the detriment of Russian science.

After having encouraged foreign funding and cooperation with researchers abroad during Boris Yeltsin's presidency, towards the end of President Vladimir Putin's second term the authorities seemed to be dissuading Russian scientists from foreign contacts. Such a development, if it continued, would also most probably have a negative effect on the inclination of foreigners who have vital knowledge to work in Russia, if they perceive that they are regarded as intelligence threats.

It would also run counter to President Dmitrii Medvedev's officially expressed opinions, mentioned above, about the importance of inviting foreign specialists to assist in the creation of the scientific-technological centres for the development and commercialisation of contemporary technologies.⁷² By undermining the cross-border flow of knowledge, counter-espionage vigilance could hamper the advance of national R&D as well as innovation.

Another unintended consequence of a strong intelligence service presence in a society is harmful behaviour on the part of intelligence officials or organisations. In a society with a less developed rule of law and institutional oversight, security service officers may fall for the temptation to make personal profit from their position. A little moonlighting may not harm national science and industry directly, but protection rackets run by domestic security service personnel and directed at small and medium-sized companies may be detrimental for the growth of innovation.

Brian D. Taylor has pointed to the negative impact on Russian society of widespread illegal activity, such as *kryshovanie* ('roofing', i.e. protection) and forced takeovers, within the Russian so-called power ministries, including the intelligence services. 'The problem is not simply one of

⁷² President of Russia (2010a) 'Dmitrii Medvedev provel soveshchanie po voprosu sozdaniia v Rossii sovremennogo tsentra issledovaniia [Dmitrii Medvedev held meeting on the issue of creating a modern scientific centre in Russia]', on the Internet: <http://news.kremlin.ru/news/7061> (retrieved 24 March 2010).

corruption, defined as the use of public office for private benefit. More fundamental is the systemic nature of the commercialisation of the power ministries, in which [...] illegal activity is viewed as normal by all parties', Taylor asserted in 2007.⁷³ In the early 21st century, the business climate in Russia arguably suffered from illegal activities by intelligence officers.

Finally, the presence of former intelligence officers in top managerial positions within Russian high technology industry could have negative implications for the development of domestic science and technology. In this aspect, the French scholar Thomas Gomart's remarks are worth noting:

Moreover, the FSB's increased influence may prove to be counter-productive in terms of economic modernisation and industrial restructuring. Despite its self-confidence, the FSB is scarcely prepared to manage all the industrial complexes with international standing. This last point is crucial, as it implies that the FSB is hampering the Kremlin's efforts at economic modernisation through national champions. This is less a conscious desire to block these efforts than a profound inability to accept the inevitable consequences of a market economy (not in terms of personal gain but in terms of the entrepreneurial spirit, risk taking and opening up to the world).⁷⁴

Russian R&D could benefit from the state's intelligence agenda to support the development of national science and industry. However, there is also a potent risk of Russian R&D suffering from various forms of intelligence service support, not only by illegal activity and deliberate attempts to promote personal and financial interests, but perhaps even more by incompetent managers recruited from the intelligence services and an obsession with security. Furthermore, it could also direct attention from the necessary process of establishing an environment in Russian society and economic life that promotes innovation, research and development, as well as entrepreneurship and the will to modernize existing and create new sustainable industries.

⁷³ Taylor (2007) *Russia's Power Ministries: Coercion and Commerce* (Syracuse, NY, Syracuse University, October 2007), p. 44.

⁷⁴ Gomart, *Russian Civil-Military Relations*, pp. 57–8.

Industrial espionage – a promising short cut or a dead end?

In conclusion, industrial espionage may seem like a promising short cut at a time when Russia feels that it is pressed to develop its science and industry rapidly in order to catch up with the West. There is little doubt that Russia in 2010 possessed the tools for extensive collection of S&T intelligence abroad, but faced apparent problems at the receiving end. An underdeveloped industrial infrastructure and the lack of a satisfactory business and innovation climate obstructed a successful transfer of know-how from Russian intelligence services, no matter how efficient they proved.

There are also operations security aspects that hamper efficient science and technology transfer. Industrial espionage could, in other words, do more harm than good. On top of this there are the intentional and unintentional consequences of a strong intelligence service presence in Russian society – the parasitic tendencies of commercialisation within the intelligence services and of industry managers with a mindset that is not conducive to the development of science and industry.

Furthermore, in an era of technological globalisation, international cooperation is of the utmost importance for scientific and technological progress. Conducting industrial espionage and counter-espionage could prove harmful to Russia by raising barriers both inside and outside Russia to cooperation with foreign scientists, engineers and businessmen.

If intelligence service support to Russian science and industry stifles, rather than boosts, development, this will have negative consequences for Russian society in general. It would undermine economic development and thus be damaging to the prosperity of Russia. The many efforts of the Russian Government to stimulate domestic R&D in the early 21st century have arguably had one main driver – to generate the economic and material resources needed to counter internal and external security threats.

The country's economic potential was the centrepiece in the Russian Federation National Security Strategy presented in May 2009 and its predecessor, the National Security Concept of the year 2000.⁷⁵ Strong state finances allow the Russian Government to stabilise society and secure control over Russia's many regions, as well as funding Russia's armed forces and the national defence industry. There are, however, well-founded apprehensions that intelligence service support to Russian science and industry could prove to be a dead end rather than a short cut to modernisation.

Finally, it is worth pointing out that Russian industrial espionage directed at foreign industry and research institutions could have security policy consequences. If they are discovered and assessed as harming other countries' national interests, intelligence operations in support of Russian R&D could result in a setback in relations between Russia and the countries concerned.

Furthermore, the security policy of smaller European states is indirectly affected by the relationship between the Russian Federation and Western great powers, most notably the USA. Uninterrupted Russian S&T intelligence gathering directed at American targets would most probably contribute to perpetuating the Cold War legacy of antagonism, or at least deep-seated suspicion, in the relations between the USA and Russia.⁷⁶ Continued mutual distrust between Russia and the USA would, in turn, negatively affect European security.

⁷⁵ Russian Federation (2009) 'Strategiia Natsionalnoi Besopasnosti Rossiiskoi Federatsii [National Security Strategy]': see e.g. paragraph 25. Russian Federation (2000b) 'Kontseptsiiia Natsionalnoi Bezopasnosti Rossiiskoi Federatsii [National Security Concept of the Russian Federation], otverzhdena, Ukazom Prezidenta, Rossiiskoi Federatsii, ot 17 dekabria 1997 g. no 1300, (v redaktsii Ukaza Prezidenta, Rossiiskoi Federatsii, ot 10 Yanvaria 2000 g. no 24)', Russian Federation Security Council, on the Internet: http://www.scrf.gov.ru/documents/decree/2000_24_1.shtml and <http://www.russiaeurope.mid.ru/RussiaEurope/russiastrat2000.html> (English) (retrieved 3 February 2005).

⁷⁶ C.f. Sibley, *Red Spies in America*, p. 175 and 248.

References

- Ackerman, Robert K. (2009) 'Threats Imperil the Entire U.S. Infostructure', *SIGNAL Magazine, AFCEA International Journal*, July 2009, on the Internet: http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2001&zoneid=77.
- Almquist, Peter (1990) *Red Forge – Soviet Military Industry Since 1965* (New York, Columbia University Press).
- Andrew, Christopher and Gordievsky, Oleg (1990) *KGB – The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (London, Hodder & Stoughton).
- Andrew, Christopher and Mitrokhin, Vasili (1999) *The Mitrokhin Archive* (London, Penguin Press).
- Appelbaum, Anne (2003) *Gulag: A History* (London, Penguin Group).
- Barron, John (1974) *KGB – The Secret Work of Soviet Secret Agents* (New York, Reader's Digest Association).
- Blank, Stephen J. (2007) *Rosoboroneksport: Arms Sales and the Structure of Russian Defence Industry* (Carlisle, PA, Strategic Studies Institute, U.S. Army War College, January 2007).
- Brogan, Benedict (2007) 'Soaring Number of Russian and Chinese Spies Diverting MI5 Attention from Terror Fight', *Daily Mail*, on the Internet: <http://www.dailymail.co.uk/news/article-491830/Soaring-number-Russian-Chinese-spies-diverting-MI5-attention-terror-fight.html> (retrieved 27 January 2009).
- Bundesamt für Verfassungsschutz (2009) *Verfassungsschutzbericht 2008* (Berlin, Bundesministerium des Innern).
- Dziuba, Sergei (2010) 'Sharashkina kontora [Sharashka's office]', *Novaya Gazeta*, on the Internet: <http://www.novayagazeta.ru/data/2010/003/00.html> (retrieved 20 April 2010).
- Gomart, Thomas (2008) *Russian Civil-Military Relations: Putin's Legacy* (Washington, D.C., Carnegie Endowment for International Peace).
- Heickerö, Roland (2010) *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm, Swedish Defence Research Agency (FOI), March 2010).
- Holloway, David (1994) *Stalin and the Bomb* (New Haven, Yale University Press).
- Interfax (2008) 'Foreigners Seeking High-tech Secrets in Saratov Region – Security Chief', Interfax News Agency (redistributed by BBC Monitoring Service).
- Kouzminov, Alexander (2005) *Biological Espionage: Special Operations of the Soviet and Russian Foreign Intelligence Services in the West* (London, Greenhill Books).
- Lefebvre, Stéphane (2007) 'Russian Intelligence Activities in Canada: The Latest Case of an "Illegal"', *Journal of Slavic Military Studies*, Vol. 20, pp. 549–58.
- Leijonhielm, Jan et al. (2002) *Den ryska militärtekniska resursbasen: Rysk forskning, kritiska teknologier och vapensystem [Russian Military-Technological Capacity: Russian R&D, Critical Technologies and Weapon Systems]* (Stockholm, Swedish Defence Research Agency).
- Lekarev, Stanislav (2001) 'Dva vida possiiskoi razvedki unifitsiruiutsia [Two types of Russian intelligence be unified]', *Nezavisimoe Voennoe Obozrenie*, on the Internet: http://nvo.ng.ru/spforces/2001-08-31/7_unification.html (retrieved 10 March 2010).
- McAfee (2009) *Virtual Criminology Report 2009*, McAfee, Inc.
- Nezavisimaia Gazeta (2010) 'V golubom vertolete [In the blue helicopter]', *Nezavisimaia Gazeta*, on the Internet: http://www.ng.ru/titus/2010-03-11/1_filantropia.html (retrieved 17 March 2010).
- President of Russia (2010a) 'Dmitrii Medvedev provel soveshchanie po voprosu sozdaniia v Rossii sovremennogo tsentra issledovaniia [Dmitrii Medvedev holds meeting on the issue of creating a modern scientific centre in Russia]', on the Internet: <http://news.kremlin.ru/news/7061> (retrieved 24 March 2010).
- President of Russia (2010b) 'Vstrecha s pobediteliami shkolnykh i studenticheskikh olimpiad [Meeting with participants in the pupil and student olympiad]', on the Internet: <http://www.kremlin.ru/news/7139> (retrieved 24 March 2010).

Racheva, Elena (2007) 'Space as Evidence', *Novaya Gazeta*, on the Internet: <http://en.novayagazeta.ru/data/2007/94/07.html> (retrieved 20 April 2010).

RF Ministry of Defence 'Polozhenie "O Generalnom shtabe VS RF" [Decree "On the General Staff of the Armed Forces of the Russian Federation"]', on the Internet: <http://www.mil.ru/847/852/1153/1339/1826/index.shtml> (retrieved 20 March 2010).

Rich, Vera (2007) 'Scientist Scientists? Risk Prosecution', *Times Higher Education*, on the Internet: <http://www.timeshighereducation.co.uk/story.asp?sectioncode=26&storycode=207675> (retrieved 25 March 2010).

Rosneft official website: <http://www.rosneft.com>.

Russian Federation (1995) Federalnyi zakon 'O vneshnei razvedke' [Federal Law 'On Foreign Intelligence'] No. 5-F3.

Russian Federation (2000a) 'Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii [Information Security Doctrine of the Russian Federation]', Russian Security Council, on the Internet: <http://www.scrf.gov.ru/documents/5.html> (retrieved 30 March 2010).

Russian Federation (2000b) 'Kontsepsiia Natsionalnoi Bezopasnosti Rossiiskoi Federatsii [National Security Concept of the Russian Federation], otverzhdena, Ukazom Prezidenta, Rossiiskoi Federatsii, ot 17 dekabria 1997 g. no 1300, (v redaktsii Ukaza Prezidenta, Rossiiskoi Federatsii, ot 10 Yanvaria 2000 g. no 24)', Russian Federation Security Council, on the Internet: http://www.scrf.gov.ru/documents/decree/2000_24_1.shtml and <http://www.russiaeurope.mid.ru/RussiaEurope/russiastrat2000.html> (English) (retrieved 3 February 2005).

Russian Federation (2009) 'Strategiia Natsionalnoi Besopasnosti Rossiiskoi Federatsii do 2020 goda [National Security Strategy of the Russian Federation up to 2020]', Russian Security Council, 12 May 2009 (by Presidential Decree No 537), on the Internet: <http://www.scrf.gov.ru/documents/99.html>.

Sibley, Katherine A. S. (2004) *Red Spies in America: Stolen Secrets and the Dawn of the Cold War* (Lawrence, Kansas, University Press of Kansas).

Stoecker, S. W. (1998) *Forging Stalin's Army: Marshal Tukhachevsky and the Politics of Military Innovation* (Boulder, Colorado, Westview Press).

SVR official website: <http://www.svr.gov.ru>.

Swedish Security Service (2007) 'Sakerhetspolisen 2006 [The Security Service 2006]', on the Internet: <http://www.sakerhetspolisen.se/download/18.7671d7bb110e3dcb1fd800019916/sakerhetspolisen2006.pdf> (retrieved 31 June 2009).

Taylor, Brian D. (2007) *Russia's Power Ministries: Coercion and Commerce* (Syracuse, NY, Syracuse University, October 2007).

United Aircraft Construction Corporation (OAK) official website: <http://www.uacrussia.ru/ru/>.

US Director of National Intelligence (2010) *Annual Threat Assessment of the US Intelligence Community for the Senate select Committee on Intelligence* (Washington, D.C., Office of the Director of National Intelligence, 2 February 2010).

Usdin, Steven T. (2009) 'The Rosenberg Ring Revealed: Industrial-Scale Conventional and Nuclear Espionage', *Journal of Cold War Studies*, Vol. 11, No. 3, Summer 2009, pp. 91-143.

Volodarsky, Boris (2009) *The KGB's Poison Factory: From Lenin to Litvinenko* (Barnsley, S. Yorkshire, Frontline Books).

About the author

Fredrik Westerlund is a researcher at the Division for Defence Analysis at the Swedish Defence Research Agency (FOI). He graduated in law as well as in political science from Uppsala University and pursued a career as a signals intelligence analyst before joining FOI. He has also worked at the Swedish Ministry of Defence.

At FOI, his main focus is on security policy aspects of Russian military development and civil-military relations. He also works with nuclear weapon and arms control issues, as well as with intelligence studies.

Fredrik Westerlund is the author of a number of reports on Russian military affairs and the military-industrial complex and co-editor of *Russian Power Structures: Present and Future Roles in Russian Politics* (FOI). His most recent publication in English is the chapter 'Russia's war in Georgia: lessons and consequences' in *Crisis in the Caucasus: Russia, Georgia and the West* (Routledge 2010), co-authored with Dr Carolina Vendil Pallin.

Correspondence address:

Fredrik Westerlund
Division for Defence Analysis
Swedish Defence Research Agency (FOI)
SE-164 90 Stockholm
Sweden

Email: fredrik.westerlund@foi.se

The FOI Russia Research Project website: <http://www.foi.se/rufs>

Selected FOI reports on Russia

Anderman, Karin; Hagström Frisell, Eva; Vendil Pallin, Carolina (2007) *Russia-EU External Security Relations: Russian Policy and Perceptions*, FOI-R--2243--SE, February 2007.

Bladel, Joris van (2008) *The Dual Structure and Mentality of Vladimir Putin Power Coalition: A legacy for Medvedev*, FOI-R--2519--SE, May 2008.

Harriman, David (2010) *Brussels without Muscles: Exploring the EU's Management of its Gas Relationship with Russia*, FOI-R--2969--SE, March 2010.

Hedenskog, Jakob (2008) *Crimea after the Georgian Crisis*, FOI-R--2587--SE, November 2008.

Hedenskog, Jakob & Larsson, Robert, L. (2007) *Russian Leverage on the CIS and the Baltic States*, FOI-R--2280--SE, June 2007.

Hedenskog, Jakob & Lavrenyuk, Viktor (eds.) (2007) *Comparing the Baltic and Black Sea Regions: Regional Security, Energy Security and Euro-Atlantic Integration*, FOI-R--2281--SE, June 2007.

Heickerö, Roland (2010) *Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations*, FOI-R--2970--SE, March 2010.

Holmberg, Carl (2008) *The Struggle for Bureaucratic and Economic Control in Russia*, FOI-R--2504--SE, April 2008.

Holmberg, Carl (2008) *Managing elections in Russia – Mechanisms and problems*, FOI-R--2474--SE, February 2008

Kjölstad, Henrik (2009) *White Russia – Xenophobia, Extreme Nationalism and Radicalism as Threats to Society*, FOI-R--2592--SE, April 2009.

Larsson, Robert L. (2007) *Nord Stream, Sweden and the Baltic Sea Security*, FOI-R--2251--SE, March 2007.

Larsson, Robert L. (2006) *Russia's Energy Policy: Security Dimensions and Russia's Reliability as an Energy Supplier*, FOI-R--1932--SE, March 2006.

Larsson, Robert L. (ed.) (2005) *Whither Russia? Conference Proceedings*, Strategiskt forum, nr. 15, Stockholm, FOI, September 2004.

Leijonhielm, Jan et al. (2009) *Russian Military Capability in a Ten-Year Perspective: Ambitions and Challenges in 2008 – Summary and Conclusions from a Study for the Swedish Ministry of Defence*, FOI-R--2759--SE, February 2009.

Leijonhielm, Jan & Westerlund, Fredrik (eds.) (2007) *Russian Power Structures – Present and Future Roles in Russian Politics*, FOI-R--2437--SE, December 2007.

Leijonhielm, Jan et al. (2005) *Russian Military Capability in a Ten-Year Perspective: Problems and Trends 2005 – Summary and Conclusions from a Study for the Swedish Ministry of Defence*, Stockholm, FOI Memo 1369, June 2005.

MalmLöf, Tomas (2006) *The Russian population in Latvia – Puppets of Moscow?*, FOI-R--1975--SE, May 2006.

Niklasson, Charlotte (2008) *Russian Leverage in Central Asia*, FOI-R--2484--SE, April 2008.

Oldberg, Ingmar (2007) *The Shanghai Cooperation Organisation: Powerhouse or Paper Tiger?*, FOI-R--2301--SE, June 2007.

Oldberg, Ingmar (2006) *The War on Terrorism in Russian Foreign Policy*, FOI-R--2155--SE, December 2006.

Oxenstierna, Susanne (2009) *The Russian Economy in 2009: Steep Decline Despite Crisis Management*, FOI-R--2853--SE, December 2009.

Oxenstierna, Susanne (2009) *Russia in Perspective: Scenarios of Russia's Economic Future 10 to 20 Years Ahead*, FOI-R--2774--SE, June 2009.

Roffey, Roger (2010) *Biotechnology in Russia: Why is it not a success story?*, FOI-R--2986--SE, May 2010.

Roffey, Roger (2008) *EU-Russian partnership to reduce bio-threats and fight disease outbreaks*, FOI-R--2493--SE, March 2008.

Unge, Wilhelm et al. (2006) *Polish-Russian Relations in an Eastern Dimension Context*, FOI-R--2008--SE, June 2006.

Vendil Pallin, Carolina (2005), *Russian Military Reform: A Failed Exercise in Defence Decision Making*, FOI-R--1777--SE, November 2005.

Vendil Pallin, Carolina & Westerlund, Fredrik, 'Russia's Military Doctrine – Expected News', RUFBS Briefing, No. 3, February 2010, http://www.foi.se/upload/RUFBS/RUFBS_Briefing_feb_10.pdf.

FOI reports can be ordered by:

E-mail: chrber@foi.se

Telephone: 08-555 030 51

Recent reports are available for down-load on the FOI Russia Project website: http://www.foi.se/FOI/Templates/ProjectPage_7897.aspx