NATIONAL INTELLIGENCE UNIVERSITY

RUSSIAN INTELLIGENCE

A Case-based Study of Russian Services and Missions Past and Present

KEVIN P. RIEHLE

RUSSIAN INTELLIGENCE

A Case-based Study of Russian Services and Missions Past and Present

KEVIN P. RIEHLE

NATIONAL INTELLIGENCE PRESS

The goal of the NI Press is to publish high quality, valuable, and timely books on topics of concern to the Intelligence Community and the U.S. Government. Books published by the NI Press undergo peer review by senior officials in the U.S. Government as well as outside experts.

This publication has been approved for unrestricted distribution by the Office of the Director of National Intelligence. The views expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the Office of the Director of National Intelligence, the Intelligence Community, or the U.S. Government. Authors of NI Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers authors to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

How to order this book: Everyone may download a free electronic copy of this book from our website at http://www.NI-U.edu. U.S. Government employees may request a complimentary copy of this book by contacting us at: press@NI-U.edu.

Editor, NI Press
Spring 2022
National Intelligence University
Bethesda, MD

ISBN: 978-1-932946-10-9
Library of Congress Control Number: 2022936044

CONTENTS

INTRODUCTION **7**

SECTION I: WHO **19**

Chapter 1: Historical Foundations 21

Chapter 2: Post-Soviet Development of Russian Intelligence and Security. 53

SECTION II: WHY **79**

Chapter 3: Internal Security and Counterintelligence 85

Chapter 4: Political Intelligence Collection 103

Chapter 5: Economic and S&T Intelligence 131

Chapter 6: Military Intelligence 165

Chapter 7: Covert Activities 187

SECTION III: HOW **215**

Chapter 8: Human Platforms 217

Chapter 9: Technical Platforms 235

Chapter 10: The Future of Russian Intelligence 261

ABOUT THE AUTHOR **275**

BIBLIOGRAPHY **277**

ENDNOTES **317**

INDEX **359**

LIST OF FIGURES

Figure 1. Relationship of Foreign Intelligence Activities to Internal Threat Concerns 35

Figure 2. Intelligence Organizations 36

Figure 3. Military Counterintelligence of the FSB of Russia, 1918-2003 40

Figure 4. Richard Sorge Postage Stamp, 1965 44

Figure 5. U.S. Intelligence Priority Structure 80

Figure 6. Major Terrorist Attacks in Russia Since the Dissolution of the Soviet Union 92

Figure 7. Notable Protest Actions in Russia 99

Figure 8. Comparison of Soviet and Russian Intelligence Priorities 105

Figure 9. Reported Russian Computer Incidents Targeting Ministries of Foreign Affairs 111

Figure 10. Arrests of Individuals Working in Ministries of Defense 114

Figure 11. Russian Intelligence Officers Targeting Defense Information 115

Figure 12. Russian Computer-Based Operations Targeting Ministries of Defense 117

Figure 13. Russian Intelligence Operations Targeting Elections 120

Figure 14. Cases Involving Russian Targeting of an Intelligence or Counterintelligence Service 126

Figure 15. Human Intelligence Methods Used in Economic and S&T Collection 133

Figure 16. Technical Intelligence Methods Used in Economic and S&T Collection 134

Figure 17. Corporate Intelligence Methods Used in Economic and S&T Collection 135

Figure 18. GRU Officers Who Defected or Attempted To Defect During the Cold War 167

Figure 19. Strategic Forces-related U.S. Espionage Cases 175

Figure 20. Soviet-era Active Measures Campaigns 193

Figure 21. Russian Assassination Types 202

Figure 22. Russian Calculus for Action Against Internal Oppositionists 204

Figure 23. Chechen External Assassinations Targets in the Putin Era 208

Figure 24. Officer Lines Within an SVR *Rezidentura* 232

Figure 25. Cold War-era SIGINT Defectors 237

Figure 26. SIGINT Collection Room in the Hotel Viru in Tallinn, Estonia 242

Figure 27. Management of Security Services 262

LIST OF TABLES

Table 1. Post-Soviet Civilian Intelligence and Security Reorganizations 59

Table 2. Foreign Intelligence Operations Neutralized, per Putin 86

CHARTS

Chart 1. Foreign Intelligence Service (SVR) 62
Chart 2. Federal Security Service (FSB) 66
Chart 3. Federal Protective Service (FSO) 70
Chart 4. National Guard 72
Chart 5. Main Directorate of the General Staff (GU) 74

INTRODUCTION

This book sprang from a global pandemic. When the National Intelligence University (NIU) transitioned from a traditional classroom setting to online instruction in spring 2020, NIU faculty were required to reformulate lectures to include only information that could be shared across an open video link. This initially appeared to be a daunting proposition for a course on Russian intelligence and security activities since one would assume that such information is not generally publicly available. Intelligence activities are, by nature, secret.

As I reformulated lectures on Russian intelligence, however, I came to realize that a large amount of reliable and accurate information exists in the public domain. Although not all public information is reliable and much of it exaggerates or mischaracterizes the subject, with careful selection a comprehensive picture emerges. I also realized that no single volume existed that credibly presented a complete, unbiased picture of Russian intelligence. I set out to develop a series of lectures, which now forms the basis for this book.

Some of the publicly available information used in this book is historical. Although this book is not intended to be a comprehensive history, Russian intelligence and security services today are deeply rooted in history, and Soviet-era organizational structures, practices, and priorities are still evident in Russian services and operations. Russian intelligence leaders deliberately evoke and celebrate historical precedents and players to justify Russian actions today and propagandize the Russian security state to the Russian people and the world. Consequently, a bounty of information about Russian intelligence history is available for a discerning reader to tap and use as a solid foundation for understanding the goals and concerns of today's intelligence services.

However, historical information does not tell the full story. More recent information is needed to build on that historical foundation and connect the present to the past. Fortunately for students of Russian intelligence, an abundance of recent case material illustrates the modern manifestations of historical precedents. This large quantity of publicly available information is not to Russia's benefit in most cases, and Russian leaders often cry "Russophobia," deny its existence, and spew counterclaims of foreign intelligence services threatening Russia. Still, a constant flow of arrests, diplomatic expulsions, defections, and forensic investigations yield data that richly illustrate Russian intelligence today.

BOOK ORGANIZATION

This book is based on a fusion of that historical and modern case material and is divided into four sections.

The first section answers the question **who** is Russian intelligence. Chapter 1 lays the foundation by presenting a brief history of pre-Soviet and Soviet-era intelligence and state security services over a nearly 80-year period. This history shows the establishment of patterns that continue to exist in Russian intelligence and security activities today. Chapter 2 focuses on the three decades since the dissolution of the Soviet Union, covering the tumultuous 1990s, when post-Soviet Russian intelligence was struggling to find a new path, to the Putin era, when it has found strong presidential support.

The second section answers the question, **why**, explaining the primary directions of Russian intelligence as they have developed across the Soviet era into today. The chapters are based on a categorization posited by Soviet intelligence officer Alexander Orlov (real name Leyba Feldbin), who defected to the United States in 1938. As Iosif Stalin's Great Purge raged in the Soviet Union, Orlov became convinced that he was next to be arrested or executed, so he escaped from his position with the People's Commissariat for Internal Affairs (NKVD) in Spain. Reportedly having struck a deal with the NKVD to maintain the secrecy of vital information in exchange for his and his family's safety,[1] he did not discuss his accesses and knowledge until 15 years later when, after Stalin died in 1953, Orlov published a blistering book about Stalin and the Great Purge.[2] Orlov wrote a second book in 1963 about his views on how Soviet intelligence operated.[3] He kept his secrecy agreement, never revealing several important pieces of information to which he had access, such as his connection to purges that took place during the Spanish Civil War, and criticizing other defectors who did expose such matters.[4]

Despite his incomplete, delayed, and at times self-serving revelations, Orlov's 1963 book about Soviet intelligence contains an analysis of eight Soviet intelligence "lines of operation." Although based on information Orlov had acquired prior to 1938, his typology serves to describe the organizational schema of Soviet-era intelligence that endures even today. When the Central Intelligence Agency (CIA) published an excerpt from the book in *Studies in Intelligence*, the journal editor described Orlov as "a thoughtful former insider" whose information is of "sufficient importance to warrant this special presentation for the intelligence community."[5]

Thus, the second section is organized along the eight "lines of operation" that Orlov described, which are adapted and grouped into five chapters:

Chapter 3 Internal security and counterintelligence (CI), which aligns with Orlov's category of infiltrating security agencies and intelligence services of foreign countries.

Chapter 4 Political intelligence, which Orlov called "diplomatic intelligence."

Chapter 5 Economic intelligence, economic CI, and science and technology intelligence.

Chapter 6	Military intelligence.
Chapter 7	Covert activities, encompassing Orlov's categories of misinformation, influence operations, and sabotage operations.

These five chapters also draw on cases revealed during the past two decades to illustrate how Russian intelligence continues to organize its operations along these lines of operation.

The third section answers the question, **how**, and is divided into two chapters describing the platforms that Russian intelligence and security services employ to perform their collection and covert action missions. Chapter 8 describes Russian human intelligence platforms, including legal, nonofficial, and illegal cover, along with their advantages and disadvantages. Chapter 9 discusses technical platforms, including signals intelligence, geospatial intelligence, and computer-based—or cyber—operations.

The tenth and final chapter posits a future for Russian intelligence, analyzing Russian services using the equation: threat = intent x capability x opportunity.[6] Russian intelligence services have both advantages and challenges that will affect the performance of their future collection and covert action missions, and thence the threat they pose. Russian intelligence leaders, including Vladimir Putin, publicly portray Russian intelligence as invulnerable and unstoppable, and Russian intelligence services benefit when the world parrots that propaganda line. A balanced, realistic analysis of Russian intelligence will prevent the tendency to see its practitioners as "10 feet tall and bullet proof," while simultaneously recognizing the true threat that they pose to target countries' national security.

HOW WE KNOW WHAT WE KNOW ABOUT RUSSIAN INTELLIGENCE

A treasure trove of publicly available source material informs this book. The sources of information span a wide range of Russian-origin and foreign materials. No single source should be viewed in isolation, but an aggregate analysis provides a comprehensive and credible picture of Russian intelligence: past, present, and future.

Soviet-era Intelligence Archives

Brief glimpses into Soviet and pre-Soviet intelligence archives provide valuable foundational material for studying the origins of Russian intelligence and state security. For the most part, those archives are closed to all but a few select, politically reliable Russian researchers, but some portions have made their way into the public domain, albeit in a controlled way.

In the 1960s, the CIA commissioned a study of the archives of the pre-Soviet Russian security service, the Okhrana, seeking the historical foundations of Cold War Soviet intelligence—that history continues to be informative today. The Okhrana ran external operations from its office in Paris, and the Paris archives were moved to the Hoover Institution Archives at Stanford University after the Bolshevik revolution. After the archives were opened in 1957, a CIA CI analyst studied them to learn what the Soviet Union had inherited from its Russian imperial predecessor. The CIA declassified and published that study in 1997.[7]

At the end of the Soviet era, as the Soviet policy of *glasnost* (openness) was taking hold and people were allowed to speak more freely and truthfully about dark aspects of Soviet history, Aleksandr Yakovlev, an advisor to Mikhail Gorbachev and philosophical founder of *glasnost* and *perestroika* (restructuring), led research into Soviet state security archives. Yakovlev famously presented a study before the Soviet parliament confirming the existence of a secret protocol attached to the 1939 Molotov-Ribbentrop pact—a nonaggression pact dividing eastern Europe into Nazi German and Soviet Russian spheres of influence—which the Soviet Union had vehemently denied throughout the Cold War.[8] Thousands of pages of material from Stalin-era state security archives are now available online in the Aleksandr Yakovlev Archive, including many documents that describe brutal and violent actions.[9] Yakovlev's organization, the International Democracy Foundation, also published a series of books based on Soviet-era archives, including intelligence files.[10] These works offer first-hand views into Soviet intelligence operations, policies, and organization, although Russian nationalists today criticize them for portraying a negative image of Soviet history.

During the 1990s, the Soviet government granted several researchers limited access to Soviet-era archives. Russian émigré journalist and former Committee for State Security (KGB) officer Aleksandr Vassiliev was allowed to view Soviet-era KGB archives specifically seeking information about Soviet espionage in the United States. His notes, which identify U.S. persons who cooperated with Soviet intelligence in the 1930s and 1940s, are now available online through the Wilson Center in Washington, DC,[11] and they have been the basis for several books about Soviet-era intelligence operations.[12] Separately, Oleg Tsarev, another former KGB officer, was granted access to files about Soviet intelligence defector Alexander Orlov. Tsarev teamed with British historian John Costello to publish the findings in a 1993 book, *Deadly Illusions,*[13] and with British espionage writer Nigel West in 1999 on another book from Soviet-era archives titled *Crown Jewels*, which addressed Soviet espionage in the United Kingdom (UK).[14] Because Russia's Foreign Intelligence Service (SVR) sponsored both Vassiliev and Tsarev, critics have accused them of being conduits for deliberately selective releases of information for Russian propaganda purposes.[15] Nevertheless, their work provides a brief but limited window into the information available in the Soviet archives.

Both the SVR and the Federal Security Service (FSB) have also officially, albeit selectively, published archival materials. Between 1997 and 2006, the SVR sponsored a six-volume book series, edited by former SVR Director Yevgeniy Primakov and titled *Essays on the History of Russian Foreign Intelligence*.[16] In 2004, the FSB published a book glorifying the history of military counterintelligence[17] and, in 2007, sponsored an edited volume of archival materials from the All-Russian Extraordinary Commission for Combating Counterrevolution and Sabotage (VChK or Cheka), the first Bolshevik state security service.[18] These and other similar volumes, written by KGB veterans rather than professional historians, contain highly selective, tightly-controlled materials about Russian intelligence and state security. Although they make no attempt at objectivity, portraying Soviet intelligence as a driving force for good in the world in opposition to an evil United States, they contain anecdotes and details that are not available in any other forum.[19]

Other Eastern Bloc and former Soviet states have been more forthcoming with their intelligence archives, providing additional glimpses into how the KGB operated in conjunction with its partners. Ukraine, Lithuania, Poland, Germany, and Czechia have made large amounts of former Soviet and Eastern Bloc materials available to researchers. The Ukrainian and Lithuanian governments, for example, have opened access to previously classified KGB journals and publications, such as *Сборник КГБ* (*KGB Digest*), a classified in-house journal in which KGB officers discussed operations and methods, and *Труды Высшей Школы* (*Works of the Higher KGB School*), which published studies of state security topics.[20] The governments of Czechia and Poland have declassified much of the archives of their communist-era security services.

Some Russian works since the end of the Soviet era have fixated on the topic of Russian traitors. Books recounting the lives and unhappy fates of Soviet and Russian intelligence officers who defected or were recruited as foreign intelligence service penetrations have become popular in Russia. Dmitriy Prokhorov's *What is the Cost of Betraying One's Homeland?*[21] and Vitaliy Karavashkin's *Who Betrayed Russia,*[22] for example, present Russian traitors whom Russians can claim to be the source of Russia's problems. Within these unmistakable propaganda narratives, however, are also historical facts.[23]

Memoirs

Numerous former Russian intelligence and state security officers have published memoirs revealing details of their service. Authors from across the Russian intelligence spectrum—military and civilian, legal and illegal officers—shed additional light on events during the Cold War. Among the most prominent is Pavel Sudoplatov's memoir, *Special Tasks,* which was published in 1994 in collaboration with American journalists Jerrod and Leona Schecter and portrayed Sudoplatov's interpretation of events from the 1930s to 1950s.[24] A Russian version of the book was published several years later.[25] Other retired officers—including intelligence illegals, officers sent abroad under false identities with no overt government connections—have offered glimpses into their careers.[26] These books provide a one-sided recollection of intelligence, often vaulting the author into a starring role, and some historians have criticized them for their undocumented assertions.[27] But, when combined with other sources available about the period, pieces can be gleaned to understand the actual events more clearly.

Counterintelligence Archives

Western CI archives contain large amounts of declassified Soviet-era intelligence- and CI-related materials, focusing particularly on the early Cold War. These operational and investigative collections offer insights into the priorities, people, and methods of Cold War Soviet intelligence activities, based on Western observations, and supplement the original case files from the Soviets' Eastern Bloc allies. U.S. Army Counterintelligence Corps and CIA archives show how the United States operated against Soviet and Eastern Bloc intelligence services and what CI services knew about their adversaries at the time.[28] Other countries have declassified similar CI material that contains a combination of Eastern Bloc operational files (e.g., Ukraine, Czechoslovakia, Poland), and Western CI files that show the countermeasures taken against them (e.g., United Kingdom, Canada, Australia, Netherlands, Sweden). Although these archives are historical, they shed light on the antecedents to today's Russian services and, in a few cases, show the spy-vs-spy game that played out during the Cold War through the eyes of that era's adversarial intelligence services.[29]

Press Reporting

Throughout the Cold War, espionage prosecutions, defections, and spy stories regularly appeared in both Western and Eastern Bloc press, revealing important details about Russian intelligence, although often with a propaganda or political purpose—and occasionally missing the mark. In 1972, for example, Western newspapers reported that a Soviet illegal using the name Anton Sabotka had defected in Canada. The Canadian government responded that no such person existed; however, a Canadian CI training manual did include a fictitious person with that name created from real cases for illustrative purposes.[30]

In 1985, the year that became known as the "Year of the Spy," however, a series of major Soviet-related espionage cases broke in the United States: Ronald Pelton, the John Walker ring, Randy Miles Jeffries, Edward Lee Howard, and others provided or attempted to provide intelligence to Soviet officers. The arrests and associated investigations received broad publicity and gave insights into Soviet intelligence services' methods and their priorities. Also in 1985, Vitaliy Yurchenko, a senior KGB officer, defected in Italy, providing the CIA with information that led to investigations of Pelton and Howard. Yurchenko's re-defection after only three months in the United States yielded massive press coverage of Soviet intelligence and the U.S. handling, or mishandling, of defectors.

After the dissolution of the Soviet Union, reporting about the Aldrich Ames, Harold Nicholson, Earl Pitts, and Robert Hanssen espionage cases, among others, demonstrated continuing post-Cold War Russian emphasis on collecting intelligence on the United States. Then in 2010, the FBI announced the arrests and deportations of 12 Russian illegal intelligence officers operating in the United States, whose missions were to spot and assess potential assets and to be a fallback option in case of a break in diplomatic relations (see Chapter 8).[31] Public revelations of these cases, supported by declassified FBI material, shed additional light on Russian intelligence activities. More recent cases like those of Yevgeniy Buryakov and Aleksandr Korshunov, two Russian intelligence officers arrested in New York City in 2015 and Rome in 2019, respectively, have expanded our knowledge further (see Chapter 5). Although many details remain classified, much can be gleaned from the publicly available reporting on these cases.

In the past decade, press reporting has extensively covered Russian covert operations in military and political conflict settings. Computer forensics companies have frequently reported the technical details of Russian computer-based collection and sabotage operations. Such openly available reporting can carry heavy doses of political bias and must be read in the context of overall Russian intelligence and covert activities, but this book is intended to assist with sorting through the hyperbole and political leanings and to set the context for understanding the reporting accurately.

Electronic and Human Penetrations and Defectors

Penetrations of Russian services can also teach much about Soviet and Russian intelligence. The U.S. Venona program intercepted and decrypted thousands of Soviet intelligence cables during the 1940s, identifying numerous Soviet-recruited sources and contacts inside the United States, Canada, Australia, and other countries. Some of the cables took decades to decrypt, and the program continued into the 1970s. Over 3,000 cables were declassified in the mid-1990s and are now available online.[32]

The United States and other allied countries have also recruited human sources inside Soviet and Russian intelligence services, who have provided valuable insider information about priorities, personnel, and operations. Early successes included Petr Popov and Oleg Penkovskiy, officers with the Main Intelligence Directorate (GRU) of the Soviet Armed Forces General Staff, with more recent cases including Aleksandr Poteyev, Sergey Skripal, and Oleg Smolenkov. These sources provide insights but are fragile and can easily be lost, and press reporting on their activities must be read with the understanding that much remains classified.

Intelligence defectors have been some of the most important sources of information about Soviet and Russian intelligence, providing significant insights into intelligence activities, priorities, people, and tradecraft. During the Soviet era, approximately 160 intelligence and state security officers defected to other countries. After World War II, most of them came to the United States. Defectors are different from penetrations because their escape from foreign control offers more time to debrief them in a secure setting, although their information starts to become obsolete the moment they defect.

There were several periods of history when defectors escaped in concentrated groups, such as during the Great Purge of the 1930s and in 1953–54, after Stalin's death. The most intense period of intelligence officer defections in the Soviet era came from 1987 to 1991, when dozens of intelligence officers became disenchanted with the Soviet system and offered their knowledge abroad. More than 25 other publicly known defectors—including Vasiliy Mitrokhin, Oleg Kalugin, and Sergey Tretyakov—left after the dissolution of the Soviet Union. Many defectors have chosen to publish books and articles for various reasons: to present their personal stories; to reveal damaging information about their former employer; to earn money; or sometimes, with the support of a receiving intelligence service, for propaganda. Defectors have occasionally been difficult to handle and withheld important information, and some have chosen to re-defect, as noted above in Yurchenko's case. Nevertheless, their insights, based upon their elite level of access to insider information and offered in debriefings and published works, add much to our understanding of how Russian intelligence operates.[33]

Official Russian Government Statements

Russia, more than almost any other country, looks back on its intelligence officers and agencies with pride, glorifying them with postage stamps, memoirs, official historical celebrations, and government awards. Russian government officials, especially during the Vladimir Putin era, regularly make public statements about the important role that intelligence and state security play in Russian life. Although these statements have a clear propaganda purpose, they also occasionally reveal previously unpublished information, such as the identities and careers of retired intelligence officers or past intelligence operations. For example, the United States first learned of an illegal named George Koval, who operated during the 1940s inside the U.S. Manhattan Project nuclear weapons program, when the Russian government posthumously awarded him the title Hero of the Russian Federation in 2007.[34] Such actions provide insights into past intelligence operations and into the current Russian government mindset toward intelligence.

Russia also publishes laws governing its intelligence and state security agencies, including the FSB in 1995 and the SVR in 1996, that openly provide these services with their authorities. The Russian government publishes its National Security Strategy, Foreign Policy Concept, military doctrine and strategy, and other formal policy documents, which reveal the objectives, priorities, and threat perceptions and drive the activities of Russia's intelligence and security services. Both the FSB and SVR also have public-facing web sites where the services publish press releases.[35]

These sources—carefully selected and placed in context—lay the foundation for understanding Russian intelligence activities today. This book is intended to assist in building greater awareness of the strengths and weaknesses of Russian intelligence and security services.

Kevin P. Riehle
January 2022

SECTION I

WHO

This first section provides a brief introduction to the history and foundations of Russian intelligence and security services, focusing on the aspects that have made Russian services what they are today. Russian services count their history from the early Bolshevik era, beginning on December 20, 1917, when Vladimir Lenin ordered Feliks Dzerzhinskiy to establish an extraordinary committee to protect the infant revolution. Events such as the Soviet export of revolution in the 1920s, the collectivization period of the early 1930s, the Great Purge of the late 1930s, World War II, the Cold War, and the chaos of the 1990s all factor into the identity of Russian intelligence and security services today. This identity rests on the foundation of the pre-Bolshevik Russian security service, the Okhrana, as early Soviet services borrowed much from their Tsarist-era predecessor.

These chapters are not intended to be a comprehensive recounting of the history of Russian intelligence and state security; that would require volumes. However, because Russian services portray themselves through the context of history, and the threat perceptions associated with the mythos of the "chekist" (a Russian intelligence or state security officer) remain, a brief review of history is required to understand who those services are today.

CHAPTER 1

HISTORICAL FOUNDATIONS

Before the Soviet era dawned in 1917, the Tsarist Russian empire established a state security service to root out revolutionaries and protect the Tsar. The assassination of Tsar Aleksandr II in 1881 clearly showed the need, leading his son Tsar Aleksandr III to create the Okhrana, or security force. The Okhrana was Russia's first modern secret police organization and became the foundation on which other such organizations were based.[36] In his 2020 speech commemorating the 100th anniversary of Russian foreign intelligence, Vladimir Putin noted that Russian intelligence and state security employees today are continuing the traditions not only of their Bolshevik predecessors, but also of those that served pre-revolutionary Russia.[37]

Ultimately, the Okhrana failed to neutralize its primary target, Bolshevik revolutionaries. Nevertheless, when the Bolsheviks took control in November 1917, the new regime created a security service that in many ways resembled the Okhrana, including its strong-arm tactics to repress revolt. Recognizing the heavy opposition that the Bolsheviks faced, the new leadership created the Extraordinary Commission for Combating Counterrevolution and Sabotage on December 20, 1917—a date that is still remembered today as the founding of Russian state security. The organization became known by its Russian acronym *ЧК* (ChK) and is correspondingly often called *Cheka*, a pronunciation of those letters, in English; the following year, the Bolsheviks expanded its name to All-Russian Extraordinary Commission for Combating Counterrevolution, Profiteering, and Corruption (VChK). The Cheka's duty was to perform a similar security function for the Bolsheviks that the Okhrana had done for the Tsar, and the people running the Cheka were the very people the Okhrana was pursuing before the Cheka's founding. Thus, the author of the first Cheka operational manual included details of Okhrana tradecraft, reportedly stating that, although the new organization had a different goal than "bourgeois" intelligence agencies, it needed to learn from their experience.[38]

Still, Fedor Drugov, one of the early members of the Cheka Collegium, the organization's leadership body, expressed unease with the methods that the Cheka was adopting from the Okhrana to deal with counterrevolutionaries and other undesirables. As he wrote in a Paris-based Russian émigré journal:

> Each of us felt in the depth of our souls that we were called upon to create something similar to the old Okhrana—and we were ashamed of the thought. It was completely obvious that the very character of the task before us would make it necessary to employ a system of surveillance and denunciations (of the latter, by the way, we had already accumulated quite a few). Who will fill the role of "stoolies"? On one hand, the thought sickened the revolutionaries, but on the other, such a task could only be assigned to people who were devoted to the revolution. How could that be?[39]

One of the defining similarities between the pre-Soviet state security order and its Soviet-era descendant was that both existed expressly to secure the ruling elite and its ideological path. Throughout Russian/Soviet history, Russian leaders have kept intelligence and state security under their direct control, both to exploit these services' capabilities to support the elite's needs and to prevent them from becoming a force that could challenge the elite. The Okhrana's mission was to secure the Tsar and the imperial system. After the Bolshevik revolution, the object of protection shifted to the Bolshevik leaders and the political system they established. As the 1977 history manual of the Committee for State Security (KGB) states unambiguously: "The activities of the organs of state security wholly and completely serve the policies of the Communist Party at the fundamental stages of developing the Soviet state."[40] In the post-Soviet era, Russian intelligence and state security continue to protect the interests of the Russian ruling elite, especially the modern manifestation of a Russian "tsar," Vladimir Putin.

Another key semblance between the Okhrana and Soviet state security was the focus on internal threats and their perceived foreign support—a linkage that persists today in the Russian security mindset. Using the archives of the Foreign Okhrana—exfiltrated from Paris, the center of Okhrana foreign operations, and brought to Stanford University in the 1920s—the CIA in 1960 conducted a study of the Okhrana's methods, looking for precedents and indicators of how Soviet heirs to Russian security might operate. This assumption of linkage was borne out when two KGB-era defectors, Oleg Gordievsky and Oleg Kalugin, noted that the KGB used Okhrana materials to train its officers in the 1950s and 1960s.[41]

The CIA analyst who performed the research, under the pseudonym Rita T. Kronenbitter, found both similarities and differences between the pre-Soviet Okhrana and Soviet-era state security. Focused on internal threats, both organizations used similar tactics in conducting intelligence activities and recruiting domestic sources to control the population and for counterintelligence (CI) purposes.[42] Their penetration of domestic opposition groups was aimed at reducing the threat to the regime, often presupposing a link between domestic groups and foreign powers. The Okhrana's emphasis on internal security was founded on an unwavering assumption that foreign powers were meddling in Russian affairs, and that assumption continued into the Soviet era. A 1977 KGB manual used in training new KGB employees made this point:

> By organizing sabotage of state workers, the exploiting class wanted to force the Soviet government to abandon the decisive path toward breaking the old bourgeois-landowner state apparatus: by encouraging speculation they tried to exacerbate economic ruin to drown the revolution in famine; with conspiracies and armed revolts, inspired

> by the participation of the imperialist West, the domestic counterrevolution tried to crush the power of the workers and peasants.[43]

OPERATIONAL TECHNIQUES

The similarities between the Okhrana and the Cheka, and subsequently other Soviet services, extended to the methods they used: *agents provocateurs*, disinformation, and double agents.

Agents Provocateurs

The Okhrana made limited use of *agents provocateurs:* agents who have been covertly dispatched, in the name of an adversary, to cause unrest or physical damage that can then be exploited to discredit the adversary. The Okhrana, for example, created a plot in 1890, which exploited Russian revolutionaries' eagerness to launch terrorist bombings against the Tsarist government, to convince the French government of the dangers of revolutionaries and to prove that the Tsarist government was tough on terrorists. With the help of an *agent provocateur*, the Okhrana created a fictitious plot to assassinate Tsar Aleksandr III, convened a group of revolutionaries in Paris, and then passed the information to the French authorities, who arrested the plotters. Only the *agent provocateur* escaped, with the Okhrana's help. The ensuing trial raised awareness of the revolutionary threat in France and resulted in the neutralization of about 25 conspirators.[44]

The Soviet Union learned from the Okhrana's use of *agents provocateurs*. Like the Okhrana, the Cheka manufactured its own opposition groups to blame for violence, such as a fictitious anti-Bolshevik conspiracy, known as the "envoy's plot," in which the British adventurist Sydney Reilly played a part. The supposed plot involved a Cheka officer posing as a counterrevolutionary, who informed British and French envoys in Moscow that the Latvian regiment in the Kremlin was ready to lead an anti-Bolshevik uprising. Reilly, who at the time was working for the British Secret Intelligence Service, provided funds to the *agent provocateur*, who passed the money directly to the Cheka. When the Cheka wound up the "envoy's plot" in September 1918, it loudly and publicly proclaimed that it had "liquidated a conspiracy organized by Anglo-French diplomats," when in reality the Cheka itself had hatched the plot.[45]

The Joint State Political Directorate (OGPU), the secret police organization that succeeded the Cheka, also sent *agents provocateurs* to meet with White Russian Army General Aleksandr Kutepov in Paris. They brought him optimistic but false reports of a flourishing anti-Bolshevik underground inside Russia, leading him to declare in 1929, "Never have so many people come from 'over there' to see me and ask to collaborate with their clandestine organizations."[46] Kutepov fell further victim in 1930 when he became the target of an OGPU kidnapping and died during the operation.[47] By the following year, Soviet provocations had burned Western intelligence services multiple times, and the possibility that the Soviet Union would use defectors as *agents provocateurs* led Western governments to question even legitimate defectors; when Georgiy Agabekov (real name Arutyunov) defected in 1930, the British Home Office initially assumed his defection was fake and he was a provocation.[48]

The Soviet state security system perfected the use of *agents provocateurs*, using them on its own people to identify anti-regime elements. In 1918, the VChK created the *Особый Отдел* (Special Section; OO) to protect against what the Bolshevik regime perceived as internal and external threats to Soviet military units.[49] The OO, which eventually transformed into the KGB Third Chief Directorate and later the FSB Military Counterintelligence Service, used *agents provocateurs* among Soviet forces to identify discontent and oppositionist sympathies. For example, Vadim Shelaputin, an officer with the Main Intelligence Directorate (GRU) of the Soviet Armed Forces General Staff, noted after his defection in 1949 that the Ministry of State Security (MGB), the post-World War II predecessor to the KGB, had embedded an officer in the office where he worked. The clandestine MGB officer would try to provoke opposition by telling anti-Soviet jokes and then asking others if they knew any.[50] Later in the Soviet period, the KGB Fifth Directorate, which was responsible for repressing opposition to Communist Party rule, used *agents provocateurs* pretending "sympathy to the cause" to infiltrate dissident groups and implicate oppositionists.[51]

Disinformation

Soviet intelligence and state security services also modeled their disinformation efforts on the Okhrana's tactics, particularly noted for planting media stories to confuse Russia's enemies and lure them into traps and to support the bona fides of agents. The Okhrana, for example, planted stories in Western newspapers detailing terrorist attacks inside Russia to convince Western intelligence services of the revolutionary threat and to corroborate agent reporting. Attacks were staged to appear serious but to cause little real damage. Disinformation also facilitated the Tsarist government's control over its population and countered foreign adversaries by regulating the flow of information citizens received.[52]

Similarly, the Soviet services extensively used disinformation to support Soviet foreign policy objectives and manipulate foreign perceptions. Soviet intelligence organizations created elaborate disinformation plots that exposed anti-Soviet sentiments while also obscuring other Soviet influence activities. Petr Mikhailovich Karpov, the first OGPU officer to defect to the West, described OGPU disinformation operations in the early 1920s that were designed to create the public image of anti-Bolshevik émigrés as anti-Semitic and to blame monarchist and White Army forces for pogroms in Russia that, in reality, were perpetrated by Red Army soldiers and Bolsheviks.[53]

Karpov himself was caught in an OGPU disinformation operation after his defection in 1924. German authorities arrested Karpov in 1929 and accused him of counterfeiting Soviet intelligence documents and selling them to the press. Among the documents that Karpov and his partner Vladimir Orlov sold was a set claiming to show that two American senators, William Borah and George Norris, had each received $100,000 from the Soviet regime for their advocacy of pro-Moscow policies in Washington.[54] One of the Soviet Union's strategic objectives in the mid-1920s was to convince a reluctant United States to extend diplomatic recognition to the Soviet regime. Recognition was a hotly debated topic in Washington, and Borah and Norris advocated for it. Dmitriy Prokhorov, a Russian historian of Soviet intelligence, claims that Karpov and Orlov's documents were actually part of an elaborate and risky deception operation run by the OGPU station in Berlin, codenamed

Фальсификатор (Falsifier), to discredit Orlov, whose "anti-Soviet activities had caused headaches in Moscow," and neutralize Karpov. The operation also simultaneously insulated Borah and Norris from accusations of Soviet manipulation. According to Prokhorov's version of events, Karpov's funds had run dry since his defection, and he approached the Soviet embassy offering to sell his services. The embassy reportedly used him as an unwitting conduit for fabricated documents that a court would assuredly rule as fakes, thereby publicly disproving the allegations contained in them.[55] While American historian Richard Spence provides some reason to suspect that Soviet influence agents had at least inspired Borah's pro-Soviet positions, the court case deflated public accusations that he had taken money to advocate for diplomatic recognition.[56]

Vasiliy Mitrokhin, a KGB officer who defected in 1992, defines the purpose of Soviet-era "active measures" as being "to create conditions favorable to the successful implementation of the Soviet Union's foreign policy."[57] Thomas Rid, in his book *Active Measures*, details numerous disinformation campaigns during the Soviet and post-Soviet era, from the 1920s to the 2000s, that involved planting press stories, creating front groups, and leaking doctored stolen classified documents to cast a negative light on the United States and its allies. In line with Mitrokhin's definition, Rid discusses Soviet and Eastern Bloc operations, including invoking extreme right-wing and racist narratives to divide populations in Europe, the Middle East, and North America,[58] and others that played both sides of the political divide in Germany to support the Soviet Union's and Russia's foreign policy objectives. Nuclear and military policies of the West were frequent targets of Soviet-era disinformation.[59] Revelations of Russian disinformation operations as recently as the 2010s show a continuing heritage from the Okhrana days, through the Soviet era, to today.

Double Agents

The Okhrana and Tsarist-era Russian military intelligence also used double agents, often captured adversary agents who were turned or coerced into approaching their original sponsors while reporting back to a Russian handler. Double agents helped to identify adversary agent handlers and served as a conduit for disinformation directly into the adversary's decisionmaking apparatus. When the Okhrana arrested agents of revolutionary organizations, it would often try to double them back, using either threats of exile to Siberia or incentives.[60] An example of Tsarist-era Russian military intelligence's cultivation of double agents began when Jose Maria Gidis approached a Russian military officer in China in 1904 and offered to provide information about Japan, which at the time was one of Russia's primary external enemies. The Russian officer suspected Gidis of contact with Japanese intelligence but cautiously accepted him and received military intelligence from him, eventually gaining control of the operation and doubling him back against the Japanese just before the outbreak of the Russo-Japanese War.[61]

The Cheka similarly realized the value of double agents during the Russian Civil War, famously in Operation *Trest* (Trust), through which the Cheka identified and neutralized Europe-based, anti-Bolshevik activities. *Trest* began when the Cheka intercepted a November 1921 letter from a Russian monarchist agent, Aleksandr Yakushev, who advocated that revolt against the Bolsheviks needed to be organized inside Russia, not by émigrés. The Cheka arrested Yakushev and turned him, using his own opinions and probably also threats, to persuade him to support their efforts against foreign-based counterrevolutionary activities. *Trest* created a fictitious anti-Bolshevik organization called the Monarchist Organization of Central Russia (MOTsR), whose members purportedly included Soviet officials who were ready to overturn the Bolshevik regime. The operation ran from 1921 until early 1927, when another double agent, Aleksandr Upeninsh (aka Eduard Opperput) turned himself over to émigrés and informed them that MOTsR was controlled by Soviet state security.[62] *Trest* caused irreparable damage to the morale and capabilities of the anti-Bolshevik movement in Europe. Vladimir Burtsev, an anti-Soviet activist in Europe, wrote in December 1927, "at this distance it is practically impossible to know which of these persons are working for and which against the Bolsheviks, and still more difficult to know which may be supporting Stalin against the Opposition, and which the Opposition against Stalin."[63]

The primary differences between the Okhrana and its Bolshevik successor organizations were the organizational scale and unbridled Soviet-era power of state security, especially during Stalin's reign. Although the Okhrana did not hesitate to use brutal and deceptive methods, it was not authorized to conduct summary executions based solely on a state security ruling, as Stalin-era organizations were. During the collectivization period of the late 1920s-early 1930s, and then again during the Great Purge of the late 1930s, Soviet state security organizations arrested hundreds of thousands of people and either exiled them to corrective labor camps or summarily executed them. That unbridled power was reined in somewhat after Stalin's death. Nevertheless, in the wake of the Prague Spring in 1968, which raised alarms among Soviet leaders that democratic forces could threaten Communist rule, the KGB created an entire directorate, the Fifth Directorate, dedicated to suppressing internal dissent and removing ideological opponents, although more often by exiling them or forcibly placing them into psychiatric institutions than by killing them. Russian services today do not exercise the same unlimited power that Stalin-era services did, although the suspicious deaths of journalists who have written unflatteringly of the Putin regime, as well as the attempted assassination of prominent Russian oppositionist and anti-corruption activist Aleksey Navalny in August 2020, suggest that killing opponents is returning as a state security method.

INTERNAL VS. EXTERNAL THREAT

Although in the West we think of Russian intelligence most often as the foreign intelligence arm of the Russian government, the core mission of Russian intelligence and state security, from the Okhrana to today, is to neutralize threats to the Russian regime itself. Thus, even the external manifestations of Russian intelligence are tied to internal security, in what John Dziak, author of *Chekisty: A History of the KGB*, called a "counterintelligence state."[64]

The Cheka's first name, the Extraordinary Commission for Combating Counterrevolution and Sabotage, encompasses that security role. In 1918, the Bolshevik regime expanded the name to All-Russian Extraordinary Commission for Combating Counterrevolution, Profiteering, and Corruption (VChK). Counterrevolution remained a major element of the Cheka's mandate, and criminal activities, such as profiteering, contraband smuggling, and extortion, were all viewed as efforts to destroy the Bolshevik revolution, unless the Bolsheviks themselves were conducting them. This internal focus predominated during the Russian Civil War, when the existence of the Bolshevik regime was at risk from those who opposed the 1917 Bolshevik coup.

As the Bolsheviks began to prevail in the civil war and push anti-Bolshevik forces out of Russian territory, Bolshevik state security increasingly began to look outward to those foreign powers that were harboring or actively supporting the anti-Bolshevik resistance. These efforts, like Operation *Trest*, were still focused on internal security but broadened the security circle to unmask counterrevolutionary groups wherever they were, founded on the premise that internal threats invariably had external sponsorship.

As the Bolshevik regime struggled to consolidate power, it was forced to rely on non-party members to fill the ranks of the Workers and Peasants Red Army (RKKA), as the Bolshevik military force was called. Some of these recruits either volunteered for the money or were coerced into supporting the Bolshevik cause, and thus were not fully reliable troops. Occasionally White forces planted agents to penetrate the RKKA and bring it down from the inside. The RKKA especially lacked a trained officer corps and was forced to rely on former imperial officers as "specialists" to lead the troops. Beginning in 1918, the mission of the VChK's Special Section (OO), and later of the KGB's Third Chief Directorate, was to identify and root out unreliable officers and troops inside the Soviet Union.

The Cheka founded the International Department (INO) in 1920 with the goal of exposing "counterrevolutionary organizations on the territory of foreign states engaged in subversive activity against our country."[65] Thus, although the INO operated internationally, its initial focus was internal. During its early years, the INO ran multiple operations directed toward unveiling foreign-based Russian émigré plots directed toward weakening or overthrowing Bolshevik rule.

In May 1922, the OGPU established the Counterintelligence Directorate, based on the assumption that foreign intelligence services were trying to infiltrate the Bolshevik regime.[66] By 1922, as the Russian Civil War was winding down, Bolshevik state security forces could start turning their attention outward, more toward foreign sponsorship of internal threats. According to OGPU defector Georgiy Arutyunov (aka Georgiy Agabekov), the Soviet leadership saw a foreign hand behind many anti-Soviet plots inside Soviet territory. For example, Soviet intelligence believed that the British were supplying weapons and money to Central Asia *Basmachis* (resistance fighters) to fight against Bolsheviks in Turkestan,[67] and the OGPU saw nefarious motives in any British move in South Asia.[68] While there was truth to a few of these suspected foreign-sponsored plots, and the British did run some intelligence operations in Central Asia,[69] the Soviet leadership was engaging, at least in part, in mirror imaging. Soviet leaders were sponsoring revolutions abroad, so they assumed that foreign powers were hatching revolutionary plots inside the Soviet Union, too.

SUPPORT TO FOREIGN REVOLUTIONARY MOVEMENTS

Marxist-Leninist ideology held that the Soviet revolution was just the beginning of a worldwide revolution to bring down capitalism. Consequently, the same agencies tasked with preventing counterrevolution within Russia were also assigned with catalyzing revolution abroad. In the wake of the Bolshevik revolution, the new Soviet government saw little need for diplomacy and operated under the philosophy that communist revolutions would quickly spread around the world and that the only foreign ties the Bolshevik regime needed would be to support that process. The *Narkomindel* (People's Commissariat of Foreign Affairs) initially ran revolutionary propaganda and communist support activities through its subordinate Bureau of Revolutionary Propaganda, simultaneously with overt diplomacy. The Council of People's Commissars allocated two million rubles in late December 1917 (approximately $4 million in current U.S. dollars)[70] to support the international revolutionary movement, with decisions on its disbursal left to the *Narkomindel*.[71] Lev Trotsky, the first People's Commissar of Foreign Affairs, is purported to have said that he would "issue a few revolutionary proclamations and then shut up shop." Although Trotsky later disclaimed those words, maintaining they exaggerated his views, he did acknowledge that diplomacy was not the "center of gravity" of Soviet activities.[72]

The higher priority was to support foreign communist parties and accelerate their efforts to establish Soviet-style governments. Although the Soviet Union disavowed control over the Communist International (Comintern)—indeed the Comintern exercised a degree of independence[73]—multiple defectors revealed a Soviet hand in numerous Communist revolutionary movements throughout Europe and Asia. For example, Samuel Ginzberg (aka Walter Krivitsky) and Ignatiy Poretskiy (aka Ignace Reiss), who defected in 1937, were directly involved in covert Comintern-sponsored propaganda activities in Poland that mixed with conventional military operations in an attempt to overthrow the Polish government during the Polish-Soviet War in 1919–20. Defectors' revelations provided an unambiguous picture of covert Soviet monetary, weapons, and intelligence support to communist revolutionary movements in Germany (1919 and 1923), Hungary (1919), Persia (1920), Estonia (1924), Bulgaria (1925), and Latvia (1928–30).[74] The OGPU and the Red Army Staff's *Разведывательное Управление* (Intelligence Department); known by the acronym *Razvedupr*) supplied money and propaganda for communists in these countries, which they used to instigate labor unrest and violent attacks hoping—in vain—to catalyze proletarian revolutions. Defectors also revealed Comintern propaganda support to Indian, Turkish, and Iranian communist parties in the 1920s, along with the OGPU's use of them for intelligence and sabotage missions. In China (1923–27) and Spain (1936–37), the Soviet Union provided extensive military aid and advisors to support its chosen side in civil wars.

During the first several years after the Bolshevik revolution, the revolutionary military nature of Comintern activities drew active *Razvedupr* involvement, while the OGPU also supported foreign communist parties for both intelligence and CI purposes. Arutyunov revealed that, until the latter 1920s, the OGPU and the Comintern had a very friendly relationship, including close association between INO head Mikhail Trilisser and chief of the Comintern International Liaison Department, Osip Pyatnitskiy. As Arutyunov wrote, "It could not have been otherwise, since the OGPU conducted operations abroad to monitor counterrevolutionary and oppositionist organizations, which included all Russian and foreign anti-Bolshevik parties, beginning with the Social Democrats and the IV International and ending with fascists. The OGPU naturally shared this information with the Comintern to facilitate its work in combating influences hostile to communism."[75] Intelligence sharing went in both directions. Soviet-era archival materials corroborate this close working relationship, as shown in a September 1922 telegram from state security chief Dzerzhinskiy to his deputy Iosif Unshlikht directing the collection of information about the background, organization, and methods of Italian fascism. Dzerzhinskiy ends the telegram, "Who do we have in Rome? Could we get this information from the Comintern?"[76]

The juxtaposition of Comintern revolutionary activities with diplomacy, however, soon became a burden, especially as the Soviet Union attempted to develop trade with foreign countries, necessitating diplomatic recognition and legitimate relations.[77] These ties particularly affected relations with the United States. In a diplomatic note written in August 1920, U.S. Secretary of State Bainbridge Colby included the connection between the Soviet government and the Comintern as one of the reasons why "it is not possible for the Government of the United States to recognize the present rulers of Russia as a government with which the relations common to friendly governments can be maintained."[78] A key Soviet concern fueling the formation of the independent Comintern in March 1919—namely, the incompatibility of conducting both conventional diplomatic relations and revolutionary appeals and propaganda from the same agency—was borne out.[79]

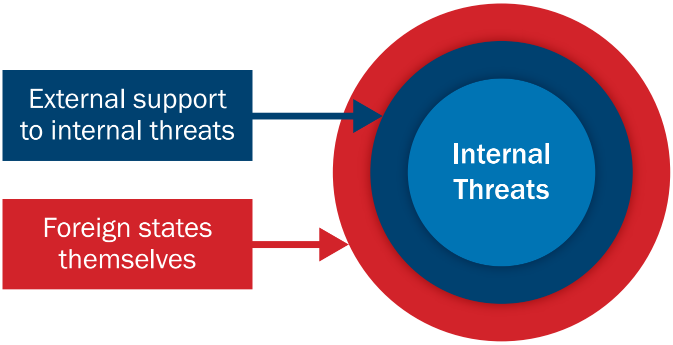
The lack of diplomatic recognition also limited Soviet intelligence services and forced them to identify other platforms for placing intelligence officers abroad. Beginning in 1918, this limitation drove the Soviet use of intelligence illegals (see Chapter 8) and also necessitated the use of other non-diplomatic platforms, such as commercial establishments, for cover. These commercial covers prominently included the All-Russian Cooperative Society (ARCOS), established in 1920 in London, and Amtorg Trading Company, established in 1924 in New York. Both companies were registered under host country laws but operated as cover platforms for intelligence operations. A defector, calling himself variously Mikhail Stein and Mikhail Hendler, offered information about Amtorg's use for intelligence cover as early as 1926, although the U.S. Government at the time did not accept his offer.[80] The British government raided ARCOS in 1927 based on suspicion that the Soviet government was using it as cover for intelligence operations.[81]

As Soviet-sponsored attempts to install communist regimes abroad in the early 1920s repeatedly failed and the resulting blowback impeded Moscow's efforts to secure diplomatic recognition, these failures ushered in a trend away from using the Comintern as an arm of Soviet foreign policy. Soviet clandestine agitation operations shifted to what former *Razvedupr* officer Ginzberg/Krivitsky labeled "decomposition work," which consisted of instigating pro-Soviet agitation in capitalist countries' governments and military forces.[82] These operations included instructions to communist parties around the world to promote the image of Stalin as the brilliant heir to Marx and Lenin and as the only leader to whom the world should look for guidance and peace. The target shifted from countries where the Soviet Union hoped to facilitate the installation of communist governments to capitalist countries, where the Soviet Union endeavored to develop stay-behind espionage and sabotage networks that could disrupt those countries' ability to attack the Soviet Union. This new strategy of clandestine infiltration of capitalist governments, as opposed to overthrowing them outright, would be clearly revealed in defector reporting during the decade following World War II.

FOREIGN COLLECTION

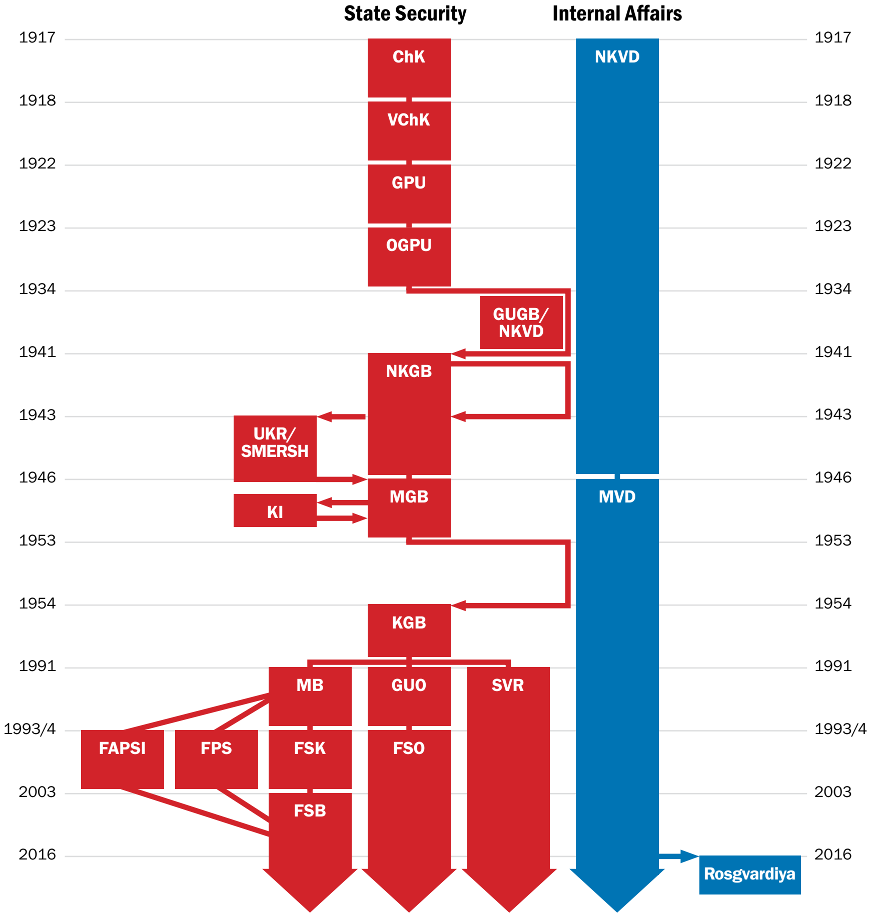
Soviet operations directed at uncovering foreign support for internal threats gradually transitioned during the 1920s to operations to collect intelligence about the foreign powers themselves, particularly their political and military intentions and their scientific and technological advancements (see Figure 1). This transition led the INO and *Razvedupr* to develop operations to penetrate other countries' foreign affairs ministries and military forces. Soviet leaders' threat perceptions determined the priority countries for these intelligence operations, with a small group of leading world powers attracting the bulk of the effort. This notion of a primary threat would eventually become known during the Cold War as the ***главный противник*** (main enemy) concept—the prioritization of Soviet intelligence and national security activities around one or two powerful adversaries that posed the greatest potential threat to the Soviet Union. Initially, if any country earned that label, it would have been Great Britain. Soviet leaders perceived British anti-Soviet plots throughout Europe and Asia, and numerous Soviet intelligence operations sought to penetrate British diplomatic facilities and recruit people capable of reporting on British political activities around the world. Other countries, such as Poland, Finland, the Baltic States, and Romania also featured high on the list of Soviet intelligence priorities during the 1920s and 1930s.

Figure 1. Relationship of Foreign Intelligence Activities to Internal Threat Concerns. Internal threats are at the heart of Soviet state security thinking, expanding to foreign connections to those internal threats, leading to intelligence activities against the foreign states themselves.


External support to internal threats
Foreign states themselves
Internal Threats

The Nazi ascent to power in 1933 brought Germany into a more prominent position among Soviet intelligence priorities and, by the mid-1930s, Germany had assumed a place alongside Great Britain as a "main enemy." Still, Stalin never abandoned hope for an accommodation with Hitler, which he achieved temporarily with the Molotov-Ribbentrop pact in 1939. In the words of one defector, Leon Helfand, "Stalin had been nibbling for an agreement with Hitler since 1933."[83]

Figure 2. Intelligence Organizations



STATE SECURITY

ChK Extraordinary Commission for Combating Counterrevolution and Sabotage

FAPSI Federal Service for Government Communications and Information

FPS Federal Border Service

FSB Federal Security Service

FSK Federal Counterintelligence Service

FSO Federal Protective Service

GPU State Political Directorate

GUGB/NKVD Main Directorate for State Security/ People's Commissariat for Internal Affairs

GUO Main Administration of Protection

KGB Committee for State Security

KI Committee of Information

MB Ministry of Security

MGB Ministry of State Security

NKGB People's Commissariat of State Security

OGPU Joint State Political Directorate

SVR Foreign Intelligence Service

UKR/SMERSH Counterintelligence Directorate

VChK All-Russian Extraordinary Commission for Combating Counterrevolution and Sabotage

INTERNAL AFFAIRS

MVD Ministry of Internal Affairs

NKVD People's Commissariat for Internal Affairs

Rosgvardiya National Guard of the Russian Federation

When Germany invaded the Soviet Union on June 22, 1941, the main enemy naturally shifted to Germany. Even before Germany was defeated, however, Soviet intelligence began targeting its wartime allies.[84] After World War II, the Soviet system initially returned to its pre-war main enemy, Great Britain, as the primary threat, but the United States soon joined Great Britain in what the Soviets called the "Anglo-American" anti-Soviet bloc. By the late 1940s, when it became clear that Great Britain was weakened economically and was losing its empire, while the United States was assuming the role of the leader of the democratic world, the Soviet Union coined the label "main enemy" and applied it to the United States. The label stuck for the rest of the Soviet era and could be said to remain in Russian intelligence minds today.

Historical Development of State Security Names

Those who study Soviet and Russian civilian intelligence and state security history often remark about the numerous name changes that the services have undergone.[85] However, those names show elements of consistency from the 1930s onward, and changes up to the dissolution of the Soviet Union reveal the ebb and flow of intelligence and state security in relation to internal security (See Figure 2).

The acronyms for Soviet and Russian intelligence and state security organizations all come from the Russian words that comprise their titles. As noted earlier, the first name given to a Soviet state security service was ChK, which stood for *чрезвычайная комиссия* (Extraordinary Commission), so named because of the extraordinary measures needed to defeat counterrevolutionaries in the Russian Civil War. The full name, which represented the organization's portfolios and subordination, was "Extraordinary Commission for Combating Counterrevolution and Sabotage under the Council of People's Commissars of the RSFSR."

In 1918, the state security organization's name was changed to VChK, adding the word *всероссийская* (All-Russian) to represent the greater reach of the organization. The full name—All-Russian Extraordinary Commission for Combating Counterrevolution, Profiteering, and Corruption—reflected the organization's priorities and the expanding threats that the Bolshevik regime faced, most of which still came from within the country. The name VChK was retired in 1922, at which time the Bolshevik leaders publicly declared victory over counterrevolution, profiteering, and corruption, and thus the end of the need for an extraordinary commission and the extralegal methods that the VChK had employed to stabilize the Bolshevik regime. However, none of the VChK's resources, roles, or missions ended. Instead, they were transferred to the State Political Directorate (GPU) under the People's Commissariat for Internal Affairs (NKVD), a temporary bureaucratic demotion for state security functions by placing them under a people's commissariat rather than directly under the Council of People's Commissars.

That demotion lasted only a short time, and, in November 1923, the organization was reinstated as an independent committee with the name Unified State Political Directorate (OGPU) under the Council of People's Commissars. The word "unified" represented a centralization of state security responsibilities under Moscow's leadership. Previously, each Soviet republic had its own GPU, staffed with local personnel and operating mostly independently. As a "unified" body, the OGPU could command state security efforts across the newly formed Union of Soviet Socialist Republics. In 1927, in an article titled "Long Live the VChK-OGPU," the Communist Party newspaper *Pravda* overtly connected the OGPU to its predecessor: "Let the word 'chekist' remain a hated word for all enemies of proletarian dictatorship."[86] The OGPU lasted with that name for a decade.

As Stalin's policies increasingly emphasized domestic political loyalty, civilian intelligence and state security functions were resubordinated in 1934 to an organization under the NKVD—this time the Main Directorate for State Security (GUGB). This resubordination marked the beginning of the Great Purge period, later called the *Yezhovshchina*, so named for Nikolay Yezhov, the People's Commissar for Internal Affairs; in 1936, Yezhov succeeded Genrikh Yagoda who had been dual-hatted as People's Commissar for Internal Affairs and Director of State Security from 1934 to 1936. A period of political repression, the *Yezhovshchina* resulted in the deaths of an unknown number of people ranging from hundreds of thousands to millions, including a large number of state security officers who were accused of being enemies of the people. The accusations were often based on little to no evidence beyond the denunciation of another jailed person, who was forced to name accomplices, whether they existed or not. Lavrentiy Beriya succeeded Yezhov in 1938, effectively ending the *Yezhovshchina.* Both Yagoda and Yezhov themselves were among those arrested and soon thereafter executed, accused by their own subordinates of being enemies of the people. The *Yezhovshchina* period left a deep scar on the Soviet psyche, effectively frightening the Soviet population into total submission to Stalin's will.

Persistent Roots in Soviet Intelligence and State Security Organizations, 1934–91

From their resubordination under the NKVD in 1934 until the end of the Soviet Union in 1991, the status of intelligence and state security functions fluctuated with Soviet political winds: sometimes subordinate to, equal to, combined with, or superior to internal affairs. The history of Soviet intelligence and state security is, in part, the history of bureaucratic battles for supremacy within the Soviet system. Throughout these shifts, however, intelligence and state security organizations were recognizable by two acronym roots:

- -VD = ***внутренние дела*** (Internal Affairs), as in NKVD and MVD.
- -GB = ***государственная безопасность*** (State Security), as in GUGB, NKGB, MGB, and KGB.

Throughout World War II, those outside the Soviet Union usually referred to the Soviet intelligence and state security with the acronym NKVD, although these entities continued to move in and out of NKVD control. Intelligence and state security functions were moved into their own People's Commissariat of State Security (NKGB) in February 1941 when Lavrentiy Beriya was promoted to deputy chairman of the Council of People's Commissars, retaining the internal affairs role. The new and separate people's commissariat was bureaucratically equal to the NKVD but was short-lived. Soon after Germany invaded the Soviet Union in June 1941, Stalin ordered the creation of the State Defense Committee to coordinate the defense of the Soviet homeland and the execution of the war, and state security was again subordinated to the NKVD. Then, in 1943, the NKGB was again separated from the NKVD and remained so until Stalin's death 10 years later.

As the Soviet Union attempted to engage less awkwardly among the society of nations in 1946, the government abandoned the organizational title "people's commissariat"—a Bolshevik phrase that had been used to describe major Soviet government elements like the NKVD and NKGB—in favor of the more conventional "ministry." Thus Soviet intelligence and state security elements and internal affairs elements were renamed the Ministry of State Security (MGB) and the Ministry of Internal Affairs (MVD), respectively.

World War II led to several short-lived exceptions to the -VD and -GB acronym naming conventions. Since 1918, military CI had been conducted by NKVD Special Sections (OOs) attached to military units as an outside control over the military's loyalty. OO officers gained a reputation for interfering in military affairs, especially during the *Yezhovshchina* when respected military officers like Marshal Mikhail Tukhachevskiy were arrested, accused of espionage, and executed. In 1943, OOs were transferred to military control under a department that was renamed the Counterintelligence Directorate (UKR) SMERSH, a portmanteau of the Russian words *Смерть Шпионам* (Death to Spies). UKR SMERSH became a feared organization during its short existence, running double agents and *agents provocateurs* inside the Soviet military to root out spies and disloyal soldiers. Several SMERSH officers defected during and soon after World War II, including Mikhail Mondich, a Czech and Hungarian interpreter who described brutal interrogations in a book published after his 1945 defection.[87] The MGB subsumed SMERSH in 1946, retaining only the acronym UKR. The SMERSH name was retired at that time, but its menace lived on in popular literature as Ian Fleming gave the name to the Soviet organization in which several antagonists worked in his James Bond series.[88]

Figure 3. Military Counterintelligence of the FSB of Russia, 1918-2003

Source: Book cover, as published by the Federal Security Service (FSB) of Russia (Moscow: Moskovskiy Poligraficheskiy Dom, 2003).

Today's descendant of the OOs, UKR SMERSH, and the MGB's UKR is the FSB Military Counterintelligence Service. In 2004, the FSB Military

Counterintelligence Service published a book regaling its history, which it counts from 1918 (see Figure 3). The book only briefly mentions the dissolution of the Soviet Union while connecting today's organization to the heroic exploits of the Soviet era.[89]

Another naming anomaly came after World War II, when the Committee of Information (KI) was created to coordinate between civilian and military foreign intelligence collection elements. The purpose of the merger, according to Vladimir and Yevdokiya Petrov, who worked in the KI before defecting in Australia in 1954, was to eliminate "wasteful duplication of effort and harmful friction."[90] KI managed civilian and military collection under the leadership of the Ministry of Foreign Affairs, and thus the KI *rezidenturas* (stations) were under the authority of an ambassador at an embassy. This arrangement lasted only from 1947 to mid-1948 when the GRU refused to share its source information and withdrew from the KI. MGB foreign intelligence components remained under the Ministry of Foreign Affairs leadership for several more years, but by late 1951 the experiment was declared over.[91]

ESPIONAGE AND SABOTAGE

The German invasion of the Soviet Union on June 22, 1941, put the Soviet Union at risk of collapsing altogether. In this environment, the Soviet tendency to merge espionage and sabotage into a single mission came to the fore, strengthening practices Soviet intelligence and state security services had implemented from the beginning of the Soviet era. Soviet intelligence activities were divided into two lines: intelligence and diversion. Initially, the intelligence directorate, led during World War II by Pavel Fitin, was responsible for collecting intelligence about Germany and its allies. The diversionary directorate, led by Pavel Sudoplatov, dispatched "intelligence sabotage" teams behind German lines to disrupt Germany's supply lines, command and control, and rear areas and to assassinate German officers. According to Fitin, the intelligence directorate supplied intelligence for the diversionary directorate, and officers were regularly exchanged between the two.[92] This crossover between intelligence and sabotage operations is a continuing characteristic of Russian intelligence services today.

Even before Germany's defeat in 1945, Soviet intelligence services, both civilian and military, began to divert some of their attention away from Germany and toward Moscow's wartime allies, reinvigorating espionage networks in Great Britain and the United States. By 1943, the GRU and NKGB had established new *rezidenturas* in places like Ottawa, Canada, and Canberra, Australia—all while conducting liaison with British and American forces in the fight against Germany. Soon after World War II, this emphasis against wartime allies transitioned into what came to be known as the Cold War.

The Soviet government, however, refused to acknowledge openly that it was engaging in espionage, claiming instead that the foreign intelligence services of adversarial capitalist states, bent on destroying the Soviet Union, were the true practioners of espionage. The 1940 version of the Soviet Political Dictionary defined "espionage" as

> one of the basic means used by capitalist nations in their fight among themselves, and in particular in their fight against the USSR. Foreign intelligence agencies began to send their spies into Soviet Russia immediately after its emergence. Foreign espionage in our country is closely tied up with diversionist and wrecking activities and is aimed at the undermining of Soviet military and industrial might.[93]

This definition was a mirror image of the Soviets' own practice, combining intelligence collection and sabotage together. The Russian narrative of being under siege by foreign intelligence services continues today.

Soviet intelligence continued operating secretly not only in foreign countries but also inside the Soviet Union during the Cold War, focusing its efforts around the "main enemy," as discussed above. News of espionage arrests and defectors going in both directions across the Iron Curtain kept Soviet intelligence at the forefront of people's minds in the West.[94] U.S. Congressional hearings frequently featured Soviet intelligence themes, and defectors appeared before Congress to openly discuss their operations against the United States. From this political climate emerged McCarthyism, named for Senator Joseph McCarthy, who conducted misguided investigations of Communist infiltration and launched unfounded recriminations and criticisms of U.S. and other countries' policies. Even popular literature and fiction reflected this Cold War focus on espionage, with *Mad* magazine's Spy vs. Spy comic strip, Boris and Natasha playing the villains in *Rocky and Bullwinkle* cartoons, and Ian Fleming's James Bond perennially fighting a Soviet counterpart.

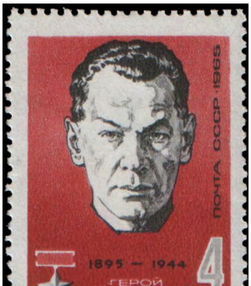
On the other side of the Iron Curtain, the Soviet Union began the postwar period honoring Soviet intelligence officers' heroic efforts in defeating the Nazi invasion. In 1947, a film entitled *Подвиг Разведчика* (*The Intelligence Officer's Deed*) appeared on Soviet and Western screens portraying a self-sacrificing Soviet officer dispatched behind German lines to infiltrate the Nazi government. The hero was reportedly modeled on a Soviet officer named Yevgeniy Khokhlov, who had conducted similar operations during the war. Unfortunately for the film maker, Khokhlov defected in Germany in 1954, dimming his heroism in Soviet eyes and possibly leading the Soviet government to replace Khokhlov with a different officer as the heroic model.[95]

Moscow's attempt to shine glory on Soviet intelligence and state security officers was not well received, however, as state security turned its attention on the Soviet people amid reinvigorated fears of internal threat. Stalin's fear of foreign infiltration through returning prisoners of war and refugees manifested itself in increased suppression of the Soviet people and strict rules against associating with foreigners. For the first several decades of the Cold War, Soviet popular media portrayed spies as foreign demons. Defectors noted that the Soviet leadership was concerned about shielding the Soviet population, especially state security officers, from the West's relative economic prosperity and political influences. With the *Yezhovshchina* not far from Soviet citizens' memories, millions more Soviet citizens were forcibly relocated, were sentenced to "corrective labor" camps, or simply disappeared. The title "chekist" became a demeaning epithet denoting a stool pigeon in the 1940s and 1950s, and Lavrentiy Beriya's arrest in June 1953 and subsequent execution further tarnished the "chekist" name.

By the mid-1960s, the Soviet government began striving to rehabilitate the image of the intelligence officer as a patriotic, self-sacrificing hero who saved the Soviet Union from fascism and continued to protect against the "main enemy." One of the first test cases for this renewed publicity policy was Richard Sorge, a Soviet illegal who operated in Japan against Germany until he was arrested in Japan in October 1941 and later executed. After years of obscurity and incriminations as a German spy, Sorge posthumously received the Hero of the Soviet Union medal in late 1964 and was featured on a Soviet postage stamp in 1965 (see Figure 4).[96] Sorge was the first in a long line of Soviet intelligence officers to be so honored, including five World War II partisan leaders and sabotage operators in 1966.

When Yuriy Andropov became KGB chief in 1967, he launched an even more aggressive public relations campaign to recover the image of the KGB officer, which was just beginning to shed the reputation of a fearful thug who knocks on the door in the middle of the night and makes people disappear. The popular TV series *Seventeen Moments of Spring*, which was based on Soviet fiction writer Yulian Semyonov's 1968 novel, appeared in 1973 and portrayed a Soviet intelligence illegal who had penetrated the Nazi military hierarchy during World War II, collecting vital information that led to the defeat of Nazism. The series became a Russian cultural staple, comparable to the prominence of the series *M*A*S*H* in the United States. Most Russians recognize the miniseries theme song, and Putin has compared himself to the quick-thinking, brave protagonist of the story, Max Otto von Stierlitz, the alias of the Soviet intelligence illegal, Vsevolod Vladimirov. The plot of the miniseries included a fictional U.S. plan to negotiate a separate peace with Germany to the Soviet Union's disadvantage,

Figure 4. **Richard Sorge Postage Stamp, 1965**



Source: Publicly available image of postage stamp issued by the Soviet Union; see, for example, https://commons.wikimedia.org/wiki/File:Dr_Richard_Sorge_spy.jpg.

framing the popular understanding of World War II among Russian citizens for decades.[97]

This popularity campaign, however, was also accompanied by increased repression driven by fear of internal threat. By the 1970s, the KGB under Andropov had created a Fifth Directorate, responsible for monitoring "ideological subversion," which was defined as internal dissent and religious activity. During the late Soviet era, the KGB played two sides of the Russian problem. On the surface, the KGB accepted and claimed to adhere to the principles of *glasnost*, and it conducted anti-dissident missions more quietly rather than openly arresting people. Some KGB officers were sympathetic with Mikhail Gorbachev's *glasnost*, *perestroika*, and *demokratizatsiya* (democratization) concepts, and they began to lose faith in their own organization. Between 1985 and 1991, over 30 Soviet intelligence officers defected; over half of them from 1989 to 1991, the densest and most sustained flow of Soviet intelligence officer defectors in USSR history, with the possible exception of World War II. These defectors demonstrated an increasing level of disenchantment with the direction that Soviet intelligence and security services were taking.

At the same time, much of the KGB's workforce was highly conservative, and many officers viewed the increasing chaos and disintegration of the Soviet Union with anger and fear. The organization became increasingly repressive while keeping its actions quiet and out of the news. That divergence finally burst into the open in August 1991, when the KGB Chairman, Vladimir Kryuchkov, emerged as one of the leaders of an anti-Gorbachev coup attempt. The failure of that coup attempt left the KGB's reputation in tatters. In a September 1991 poll of Russian citizens, only 8 percent said they trusted the KGB, while 39 percent did not trust the KGB and 18 percent did not *fully* trust the KGB. Twenty-five percent refused to respond, likely representing lingering fear that their answers could be used against them.[98]

After Kryuchkov's arrest for his involvement in the coup attempt, Gorbachev appointed Vadim Bakatin, the Minister of Internal Affairs, as KGB director. Bakatin, whom Gorbachev assigned to dismantle the KGB, wrote in 1992: "The traditions of *chekism* are to be eradicated, *chekism* as an ideology must terminate its existence. We must comply with the law, but not ideology."[99]

MILITARY INTELLIGENCE

Soviet/Russian military intelligence has followed a path parallel to civilian intelligence and state security. Organizational names have remained fairly consistent: the "RU" in GRU, which is the Russian acronym for "intelligence directorate," has persisted through Soviet/Russian military intelligence history until recently. The name GRU was officially changed in 2010 to the GU (Main Directorate), dropping the word "intelligence." Nevertheless, at the celebration of the 100th anniversary of the founding of Russian military intelligence in November 2018, Putin expressed wonder at why the name had been changed and suggested the old name, GRU, be restored.[100]

The first Bolshevik military intelligence organization, the *Registupr* (Registration Department) was created in November 1918 as an element of the Revolutionary Military Council of the Red Army. The department was tasked with coordinating army intelligence units that supported Bolshevik forces in combating counterrevolutionary forces during the Russian Civil War. In April 1921, the *Registupr* was renamed the *Разведывательное Управление* (Intelligence Department) of the Red Army Staff, often called by its Russian abbreviation *Razvedupr*. Even though the name was officially changed in 2010, most people inside and outside Russia continue to call it the GRU.

As noted above, Soviet, and now Russian, military intelligence has always had two roles: intelligence collection to support military decision-making and covert action to support Soviet political objectives. These two concepts are combined in the Russian word *razvedka,* which is usually translated into English as "intelligence." According to Ginzberg/Krivitsky, a *Razvedupr* officer who was transferred to the NKVD in 1936 and subsequently defected in 1937, the *Razvedupr* was

> charged to obtain not only the fullest possible information about a foreign army, navy, or air force, but all political and economic information which, when collated, might influence the General Staff and the Politbureau in matters of foreign policy. At one time an attempt was made to draw a distinction between military and political and economic intelligence, but it was found impossible to divorce political and economic questions from those of pure military intelligence.[101]

Mirroring civilian intelligence and internal security, the history of Russian military intelligence is filled with bureaucratic conflict, and the Soviet era saw frequent struggles between military and civilian intelligence. When Stalin took full control of the Soviet Union in 1927, trust between services began to erode. Stalin distrusted military intelligence for representing the views of his archrival, Lev Trotsky, whom Stalin exiled from the Soviet Union in 1928 and finally arranged to be assassinated in 1940. Military leaders reciprocated Stalin's mistrust. Multiple *Razvedupr* officers who defected provided information about their role in supporting Comintern-sponsored revolutionary activities. In some cases, these officers' defections came a decade after Stalin took power, when the Soviet emphasis had shifted from world revolution to "Socialism in one country"—a policy that officers who had served in the *Razvedupr* during the early Bolshevik years viewed as a betrayal of Lenin's path.

When *Razvedupr* officer Poretskiy/Reiss defected, he issued an anti-Stalinist manifesto in a letter to the Central Committee of the Communist Party, dated July 17, 1937: "The working class must defeat Stalin and Stalinism so that the USSR and the international workers' movement do not succumb to fascism and counter-revolution. This mixture of the worst opportunism, devoid of principles, and of lies and blood threatens to poison the world and the last forces of the working class." He further demanded a "return to Lenin's international!"[102] Ginzberg/Krivitsky decried that "Bolshevism, Leninism, and socialism are dead in the Soviet Union, and that no genuine attempt is now being made to carry out the teachings of Karl Marx. The Soviet Union has become a rigid dictatorship maintained by a system of wholesale purges, and Stalin is attempting to maintain his unstable position by a policy of military aggression."[103] Aleksandr Graff (aka Alexander Barmine), another *Razvedupr* defector, wrote in an open letter in December 1937: "Had I consented to remain in the service of Stalin I should have felt myself morally defiled, and should have had to take a share in the responsibility for crimes committed daily against the people of my country. It would have meant betraying the cause of Socialism to which I have dedicated my life."[104] By the mid-1930s, these attitudes were not uncommon among Lenin-era military intelligence officers.

Adding to Stalin's mistrust, the *Razvedupr* experienced a series of compromises and failures in Europe in the early 1930s, leading Soviet leadership to transfer senior NKVD officers to the *Razvedupr* to "correct" these failures in 1934.[105] In 1935, Stalin removed the long-serving *Razvedupr* chief, Yan Berzin, who had been promoted to that position just after Lenin died in 1924. At about the same time, Stalin ordered the NKVD to begin collecting military intelligence, either duplicating or edging out the *Razvedupr* in some cases,[106] and he had high-producing *Razvedupr* officers, including Ginzberg/Krivitsky and Porestsky/Reiss, transferred to the NKVD to strengthen its capabilities. Berzin returned for a short period as *Razvedupr* chief in 1937 after a deployment in the Spanish Civil War, but later that year he was arrested and accused of Trotskyism. He was executed in 1938. *Razvedupr* officers respected their leader and saw Berzin's removal from power as a strike against their profession. This sentiment was strengthened by the arrests and executions of eight senior Soviet military leaders, including Marshal Mikhail Tukhachevskiy. After their executions in June 1937, Graff/Barmine made an unguarded comment to a friend: "What on earth is happening there? This is too horrible. The best men—the flower of the Army…."[107]

Ginzberg/Krivitsky speculated that Stalin may have wanted to remove military leaders because they saw Germany as a greater threat than Great Britain, in opposition to Stalin's view.[108] Among the senior military leaders whom Stalin's purges removed were Jews who were unsurprisingly opposed to any pact with Nazi Germany. The military leadership's resistance may have impeded Stalin's efforts to reach an agreement with Hitler. That agreement finally came in August 1939 with the Molotov-Ribbentrop pact, but not until most senior military leaders, including many in military intelligence, had been purged. Ironically, when Tukhachevskiy and seven other senior military officers were arrested and executed in 1937, they were accused of espionage on behalf of Germany.

When military intelligence sources began in 1940 to report that Germany was preparing an attack on the Soviet Union, Stalin refused to believe those reports. He had the sources investigated, assuming they were British spies trying to ruin the Soviet relationship with Germany.[109] A 2006 Russian analysis of why the Soviet Union was not ready for a German attack in 1941 stated, "The main reason for the Red Army's unpreparedness to actively repel aggression was miscalculation by the political leadership in assessing the situation and indecisiveness and insufficient principles of the military leadership and leadership of the RU in 1941."[110] This analysis did not mention Stalin by name, but his views—that reports of British plotting were more believable than those of German betrayal—were reflected in a historical essay sponsored by Russia's current Foreign Intelligence Service (SVR):

> From reliable sources in London and Paris, [Soviet] intelligence received information about instructions that the governments of England and France gave to their military delegations in negotiations in Moscow, where measures to prevent aggression against Poland were being discussed. The instruction directed the delegations to stretch out the time, not to take any obligations on themselves, and not to sign any documents; in other words, to facilitate a conflict between Germany and the Soviet Union.[111]

Military intelligence quickly gained greater respect, however, when it became indispensable in fighting the invading German army. Along with the NKGB, Soviet military intelligence deployed intelligence and intelligence-sabotage groups into the German rear area to collect intelligence through human and technical means and to destroy German lines of communication. According to a Russian history of the GRU, 564 military intelligence officers were awarded the rank of "Hero of the Soviet Union" during the war.[112] Moscow elevated the status of the *Razvedupr* in 1942, bestowing the title Main Intelligence Directorate (or GRU)—a name it retained for nearly 70 years.

As the GRU tasked its sources to turn their attention to the USSR's wartime allies, collection focused on three main areas: military forces information, known today as foundational military intelligence; military-related science and technology information; and political information. Among science and technology targets, a high priority for collection was information about atomic weapons development. Several important GRU operations penetrated U.S. and British atomic weapons establishments, providing the Soviet Union with the information it needed to develop its own atomic bomb by 1949, significantly earlier than it could have done without the help of espionage. Throughout the rest of the Cold War, the GRU continued along these basic collection lines, using legal and illegal human platforms and increasing its use of technical platforms, including satellites.

By the end of the Cold War, GRU collection focused on several major themes that will be discussed in more detail in Chapters 5 and 6:

- Collecting foundational military intelligence, i.e., information about the basic elements of a foreign military force that the Russian military would face in a military conflict.
- Collecting intelligence on strategic forces, particularly nuclear weapons capabilities and strategic missile defense capabilities.
- Collecting intelligence for strategic contingency purposes, including information on an adversary's critical infrastructure to support attack planning and covert operations should Russia find itself in a war.
- Collecting intelligence about foreign military weapons research and development.

Since the dissolution of the Soviet Union, the GRU has continued to exist with little change. GRU personnel were heavily involved in conflicts in Chechnya and Georgia, and they continue to be involved in conflicts today in Ukraine, Syria, and Libya. Their mission remains similar to what it was at the beginning of the Soviet era: to collect military intelligence and to conduct covert operations.

CONCLUSION: EVOLVING PRIORITIES

Despite shifts in organizational status and name changes, the methods employed by Soviet intelligence and state security services and their subordination to the Communist Party remained consistent throughout the Soviet era. As stated in the 1959 KGB basic regulation:

> The Committee for State Security of the USSR Council of Ministers and its local bodies are political bodies, performing the guidelines of the Central Committee of the Party (CPSU) and Government on the protection of the Socialist State from attacks of foreign and domestic enemies, as well as the defense of the USSR state border. Their mission is to thoroughly monitor the secret activities of the Soviet state enemies, reveal their intentions, and prevent criminal activities of imperialistic intelligence services against the Soviet state.[113]

Correspondingly, within both the internal and external threat calculation, the focus of Soviet intelligence and state security evolved over time in line with Party priorities. KGB defector Petr Deryabin published a book with American journalist Frank Gibney in 1959 that cited a KGB aphorism: "In the *Yezhovshchina*, the god of state security sat in the political section. During the period of collectivization, god sat in the economic section. During the war, god was in intelligence and, after the war, in counterintelligence."[114] Using the image of a "god of state security," Deryabin captured the fluctuations in intelligence and state security priorities in the Soviet era.

During the early 1930s, when the Party's emphasis—at Stalin's insistence—was on the collectivization of agriculture and the industrialization of the Soviet economy, "god" sat in the economic section. The primary state security mission was to counter the internal threat that originated with millions of Soviet citizens who resisted the forced and wrenching transformation of the economy. During the *Yezhovshchina* era, the threat was also focused internally but transitioned to political loyalty, and the NKVD Political Directorate took precedence. During World War II, when the country faced a legitimate external threat, the "god" sat in intelligence, which was needed to defeat the German invasion. When the war ended, "god" returned to a perceived internal threat, represented again by the Soviet people themselves. Counterintelligence, which in the Soviet definition includes any connection between the Soviet people and foreigners, took precedence, and Soviet state security directed the bulk of its attention at the Soviet population. Several post-World War II defectors objected to this turn inward, perceiving their wartime intelligence and state security mission to be honorable and necessary in the face of external enemies; however, they could not endure the post-war mission that mandated they turn these tools against the Soviet people.

CHAPTER 2

POST-SOVIET DEVELOPMENT OF RUSSIAN INTELLIGENCE AND SECURITY

Despite an ebb in popular acceptance of the "chekist" after World War II, the concept of a "chekist mindset" continued to permeate state security functions in the Soviet Union. The apogee of the KGB's power came in 1982, when Yuriy Andropov became General Secretary of the Communist Party of the Soviet Union. No chekist had risen to that position since Lavrentiy Beriya assumed control of the Soviet government at Stalin's death in 1953, only to be arrested soon thereafter and executed. Twenty-nine years later, a chekist was in charge of the whole country. It would be 17 more years before another chekist achieved comparable standing: Vladimir Putin was a junior KGB officer in Leningrad when Andropov rose to the post of Party General Secretary.

The chekist mindset is defined by constantly perceiving threats and seeking ways to mitigate them. Threats might come from within Russia. The Russian people are potential sources of unrest that could challenge the Russian leadership. Thus, the Putin regime has endeavored to co-opt the Russian people by spreading patriotic rhetoric and controlling the information they receive, thereby preventing the emergence of popular movements that could rival him.

Threats can also come from outside Russia, such as the United States and NATO, and this view became the foundation of the "main enemy" concept during the Soviet era. Today, that same pursuit of foreign enemies is why Putin sees a U.S. hand behind "color revolutions" in the Near Abroad, why Russia has publicly accused the United States of being behind expulsions of Russian diplomats from European and other countries in 2018, and why this theme permeates Putin's rhetoric in general.[115]

Historian Julie Fedor explored the foundations of Russia's threat perception in a 2011 article that analyzed Russian conspiracy theories about the West. The most common among those conspiracies is a fictitious concept called the Dulles Plan, named for Allen Dulles, who served as the U.S. Director of Central Intelligence from 1953 to 1961. The plan outlines a grandiose plot to destroy Russia, using clandestine infiltrations into Russian society to debase the Russian people's morals and turn Russians against their own government, based on a non-existent speech that Dulles supposedly gave in 1945.[116] The plot of the 1970s Soviet TV mini-series *Seventeen Moments of Spring* reflected a related conspiracy theory, portraying Dulles—a U.S. Office of Strategic Services officer in Bern, Switzerland, during World War II—as plotting with Nazi Germans to betray the Soviet Union.[117] Fedor demonstrates that the belief in the Dulles Plan continued well into the Putin era, and that the leaders of Russia today, whose professional lives began during Andropov's time as KGB director, were immersed in the legend. As recently as May 2020, Russian Permanent Representative to the European Union (EU) Vasiliy Chizhov cited the Dulles Plan as the basis for Western criticism of Russia.[118]

In the immediate aftermath of the Soviet Union's dissolution, the Boris Yeltsin administration faced the task of figuring out what to do with the remnants of the KGB and the chekist mindset that permeated it. How could Yeltsin use or control this organ of the government that had caused so much fear during the Soviet era and had discredited itself by attempting to remove Gorbachev from power? The last KGB director, Vadim Bakatin, quickly eliminated the Fifth Directorate and went as far as revealing to U.S. Ambassador Robert Strauss the existence and locations of KGB listening devices inside the new U.S. embassy building in Moscow.[119] Strauss reported that Bakatin made this revelation out of a sense of cooperation and goodwill, with "no strings attached." Bakatin's action, however, was met with harsh criticism within the state security apparatus, including allegations of treason.[120]

The dissolution of the Soviet Union did not mean that threats to the Russian Federation ceased. The newly independent Russian Federation faced significant security threats and turned inward even more, focusing its security apparatus on legitimate concerns. These dangers included nuclear proliferation, terrorism, and organized crime, along with armed conflicts near or even inside Russia's borders in Tajikistan, Moldova, Armenia-Azerbaijan, Georgia, and later Chechnya. Russia also regretted losing the influence, especially the economic connections, that it had enjoyed in the other 14 suddenly independent former Soviet republics. Russian security services continued to perceive the need to defend Russians both inside the Russian Federation and abroad.

While some politicians, like Andrey Kozyrev, publicly advocated for removing barriers that had separated the Soviet Union from the West, especially from the United States,[121] operations targeting the old enemies of the Soviet Union continued. Bakatin lasted in position only a few months before the Soviet Union dissolved, and Soviet-era politicians who shared a mindset closer to that of the chekists whom Bakatin had tried to eradicate, succeeded him as leaders of the new Russian intelligence and security services. These officers harbored Cold War suspicions of the West, believing that forces abroad wanted to keep Russia in a state of controllable paralysis. They sought to uncover and frustrate outside attempts to influence the situation inside Russia. The chekist search for outside explanations to domestic problems survived the dissolution of the Soviet Union.

During the Yeltsin era, the guiding philosophies of Russian intelligence and security grew into concepts similar to those we see now under Putin:

- A struggle for spheres of influence in geopolitics has replaced ideological conflicts.
- Efforts must be made toward the "reconstitution of Russian statehood."

- Russia's defense capability can on no account be allowed to be weakened.
- Free access to other countries' markets must be guaranteed.[122]

Just as in the earliest days of the ChK, the chekist mindset today is constantly looking for, and sometimes fabricating, a connection between domestic threats and foreign enemies. This perceived connection makes the repression of internal dissent more acceptable to the Russian people by making it appear to be a defense against foreign invasion. For example, when prominent Russian opposition activist Aleksey Navalny released a documentary in 2015 that exposed corrupt business deals by Russia's Prosecutor General Yuriy Chayka's family members, Chayka dismissed the video as a political attack by an American businessman. When Russians protested before Putin's inauguration as president in 2016, Russian state media labeled the protesters as pro-Western, unpatriotic, and immoral.[123] The chekist mindset is at the foundation of this threat narrative that ties internal dissent to foreign powers.

The introduction to a 2013 memoir by Valeriy Velichko, a former general-major in the KGB 9th Directorate, expressed suspicions common among state security personnel about Russian leaders perceived to be under Western influence:

> Who are they? Are Yeltsin, Gorbachev, activists in the interregional deputies' group, Gaydar, Chubays, and the "father of Russian democracy" A. Sakharov, the heroes who brought an end to the "cursed totalitarian communist regime," who granted independence to the union republics, and long-awaited freedom to the Soviet people? Independence from whom and what? Or are they open traitors under the direction of the West, who destroyed a great state, stole and sold off its riches, and submerged the majority of its citizens for years of humiliating existence. No thanks to them, even now we cannot destroy the limitless criminality and rampant corruption of Russian officialdom at all levels. Wasn't it through their doings that God's commandments and the precepts of the builders of communism have been forgotten, that the basest instincts have been awakened in the masses, and

> immorality, fraud, and passion for immeasurable wealth are flourishing? Where were those all-seeing and all-knowing Andropovite chekists, whose duty it was to foresee and prevent such a tragedy?[124]

In 2010, 12 Russian intelligence illegals were arrested or indicted in the United States, representing a continuation of the Russian intelligence priority placed on the United States even in the post-Soviet era. Among the illegal officers arrested, one husband and wife couple (Mikhail Vasenkov, aka Juan Lazaro, and Vicky Palaez) had been dispatched to the United States in 1983 and continued their operations after the dissolution of the Soviet Union. Others included two husband and wife couples dispatched to the United States during the Yeltsin years: Vladimir and Lidiya Guriyev (aka Richard and Cynthia Murphy) and Andrey Bezrukov and Yelena Vavilova (aka Donald Heathfield and Tracy Lee Foley). These illegals will be covered in more detail in Chapter 8.

Mark Galeotti, an expert on Russian state security activities, has noted several manifestations of the mindset in Russia's security services to continue intelligence operations against the United States. He cites Russian intelligence and state security officers as saying:

- "If the West loses, we gain": a projection advancing a zero-sum proposition in the struggle of Russia and the West.
- "Russia is at risk": a narrative professing that the West was attacking Russia through "color revolutions" and that Maidan demonstrations in Kiev, Ukraine, were orchestrated by the CIA.
- "Better action than inaction": intelligence and state security organs have a bias toward acting, even without coordination with less aggressive organizations, such as the Ministry of Foreign Affairs.[125]

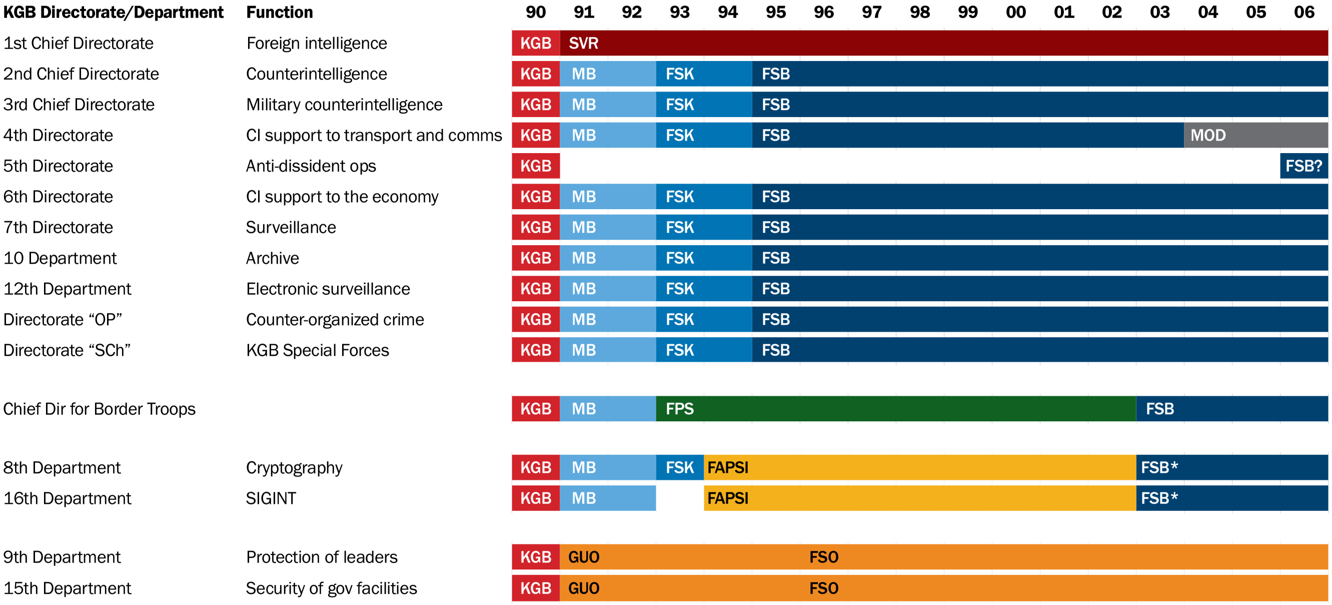
From the depths of the August coup in 1991, the chekist mindset has returned and is alive and well in Russia. Today, Russian intelligence and security officers proudly claim the title "chekist" to recall the greatness of their history. State Security Workers Day, popularly known as "Chekists Day," was reinstated as a public day of recognition in 1995. That day now is celebrated annually on December 20, the anniversary of the founding of the Cheka in 1917. In 2017, an interviewer asked FSB Director Aleksandr Bortnikov whether using the word "chekist" to refer to Russian state security workers today bothered him because of the parallels with the original VChK. He answered that it did not bother him at all. In his view, the history, experience, and tradition reflected in that title are not limited to the period of the VChK or to the time of the "avenging sword of the revolution." To deny the word "chekist" would be to "assign generations of our ancestors to oblivion."[126]

POST-SOVIET REORGANIZATIONS

When the Soviet Union dissolved and Yeltsin took charge of Russia, the Russian government took steps to break up the all-powerful KGB into several agencies. Initially, it was divided into three: the SVR, which continues its foreign intelligence mission today; the Ministry of Security (MB); and the Main Administration of Protection (GUO), which was responsible for protecting senior leaders and important government facilities. The MB contained most of the functions and personnel of the old KGB, and by 1993, Yeltsin began to realize that this renamed but still potent organization could become a threat to his governing power.[127] Reformers succeeded in persuading Yeltsin to dissolve the ministry and split the functions into three additional organizations: the Federal Counterintelligence Service (FSK) inherited the CI functions of the MB; communications security and signals intelligence (SIGINT) were transferred to the Federal Agency for Government Communications and Information (FAPSI); and the largest portion of personnel became the Federal Border Guard Service (FPS). Consequently, by 1994, five different Russian agencies conducted the missions that the KGB had previously run.

Most of the KGB-era directorates were transferred in their existing form to one of the newly founded organizations (see Table 1). Their direct descendants continue to fulfill their responsibilities today. As noted above, one exception was the Fifth Directorate, which was responsible for investigating dissent and anti-Soviet activities. This directorate caused the most fear among the Soviet population, since it investigated anti-Soviet literature,

Table 1. Post-Soviet Civilian Intelligence and Security Reorganizations



KGB Directorate/Department	Function	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06
1st Chief Directorate	Foreign intelligence	KGB	SVR															
2nd Chief Directorate	Counterintelligence	KGB	MB		FSK		FSB											
3rd Chief Directorate	Military counterintelligence	KGB	MB		FSK		FSB											
4th Directorate	CI support to transport and comms	KGB	MB		FSK		FSB									MOD		
5th Directorate	Anti-dissident ops	KGB																FSB?
6th Directorate	CI support to the economy	KGB	MB		FSK		FSB											
7th Directorate	Surveillance	KGB	MB		FSK		FSB											
10 Department	Archive	KGB	MB		FSK		FSB											
12th Department	Electronic surveillance	KGB	MB		FSK		FSB											
Directorate "OP"	Counter-organized crime	KGB	MB		FSK		FSB											
Directorate "SCh"	KGB Special Forces	KGB	MB		FSK		FSB											
Chief Dir for Border Troops		KGB	MB		FPS										FSB			
8th Department	Cryptography	KGB	MB		FSK	FAPSI									FSB*			
16th Department	SIGINT	KGB	MB			FAPSI									FSB*			
9th Department	Protection of leaders	KGB	GUO					FSO										
15th Department	Security of gov facilities	KGB	GUO					FSO										

Note: ***FSB?*** *indicates the FSB gained, as of 2005, some functions similar to those of the KGB Fifth Directorate, including investigating anti-government speech;* ***FSB**** *indicates most of FAPSI was folded into the FSB in 2003, while portions also transitioned to the SVR and the FSO.*

Acronyms

FAPSI=Federal Agency for Government Communications and Information
FPS=Federal Border Guard Service
FSB=Federal Security Service
FSK=Federal Counterintelligence Service
FSO=Federal Protective Service
GUO=Main Administration of Protection
MB=Ministry of Security
MOD=Ministry of Defense
SVR=Foreign Intelligence Service

statements, and jokes. On Vadim Bakatin's order, the Fifth Directorate was eliminated in 1991.

Commentators in the West saw this reorganization as a great improvement. The hated KGB and its repression were officially gone, and no single organization could control the new democratic Russia, they thought. However, despite agency leaders' assurances,[128] a spirit of competition arose among the five services, and failures, such as the disastrous operation to free hostages held in a hospital by Chechen separatists in Budennovsk, Stavropol Krai, in June 1995, left the services looking weak and incapable.

What is known today as the Federal Security Service (FSB) came into existence in 1995, less than a week after the Budennovsk debacle. Vladimir Putin led the FSB from July 1998 to August 1999 and saw firsthand the coordination problems that the splintering of Russia's intelligence and security services created. After being elected president in 2000, Putin began the eventual re-accumulation of state security functions that had been broken up during Yeltsin's time. The Federal Border Service was resubordinated to the FSB in 2003. FAPSI was also dissolved in 2003, with most of its functions going to the FSB and a few pieces going to the SVR and Federal Protective Service (FSO), the successor to the GUO. As of 2005, the FSB regained all but a few specialized functions that the KGB had controlled during the Soviet era, including the suspected return of functions and practices similar to those of the KGB Fifth Directorate, including investigating anti-government speech.

CONTINUING HISTORY

Russia has not forgotten its glorious intelligence past. In December 1999, then-Prime Minister Vladimir Putin said, "Bodies of state security have always defended the national interests of Russia. They must not be separated from the state and turned into some kind of monster... We nearly overdid it when we exposed the crimes committed by the security services, for there were not only dark periods, but also glorious episodes in their history, of which one may really be proud."[129] In 2005, Putin publicly used the phrase "*Бывших чекистов не бывает*" ("There is no such thing as a former chekist."). This phrase had been popular within the KGB for many years to indicate the organization's pride and elite nature, similar to when a member of the U.S. Marine Corps says, "there is no such thing as a former Marine." Putin's public use of the chekist phrase shows both his trust and reliance on state security organizations, as well as his expectation that former employees of the state security organs should remain loyal and compliant with his orders.[130]

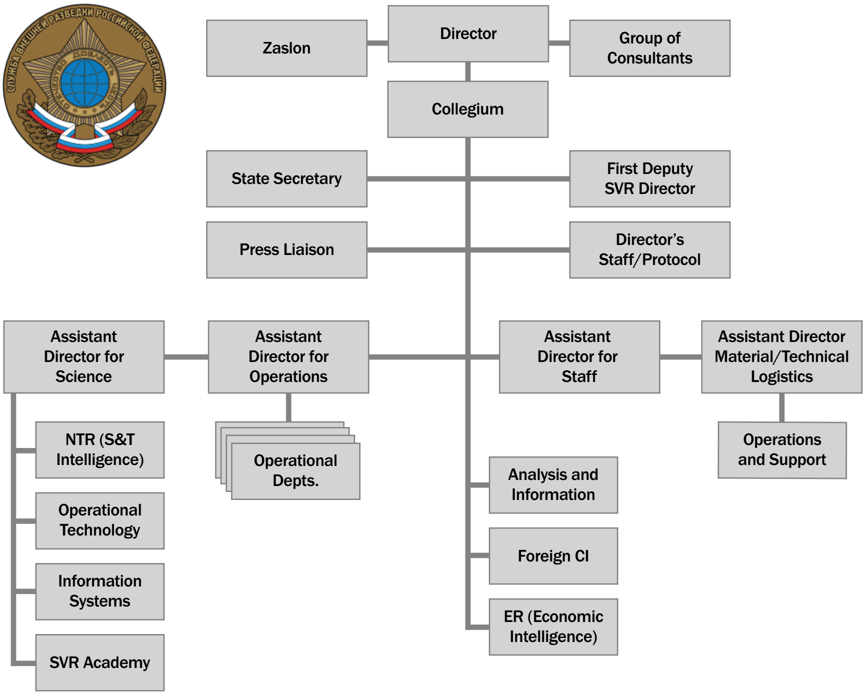
This historical continuity was evident when Russia issued a postage stamp in 2000 to commemorate the 80th anniversary of the founding of Russian foreign intelligence. The stamp lists three acronyms: INO, PGU, and SVR. These acronyms represent the names of the Russian foreign intelligence organization from its original founding under the Cheka in 1920 (International Department, INO) to the founding of the KGB in 1954 (First Chief Directorate, PGU) and the SVR today. There is no disruption in that history as far as Russian intelligence officers are concerned. During a celebration at SVR headquarters to commemorate the organization's 80th anniversary in 2000, Putin met with other former KGB/SVR chiefs—Vladimir Kryuchkov (1988–91), who had served three years in prison for his role in the August 1991 coup attempt; Leonid Shebarshin (1991); Yevgeniy Primakov (1991–96); and Vyechaslav Trubnikov (1996–2000)—as well as famous intelligence agents, including British defector George Blake. Notably absent from the attendee list was Vadim Bakatin.

Similarly, a history of the FSB Military Counterintelligence Service published in 2004 hardly mentions the dissolution of the Soviet Union. Russia also issued a commemorative postage stamp in 2017 commemorating the 100th anniversary of the founding of Russian state security. In the subsequent years, additional 100th anniversaries were celebrated: the founding of the illegals program, radio-technical intelligence (known in English as signals intelligence), border guards, counterintelligence, and foreign intelligence.

FOREIGN INTELLIGENCE SERVICE (SVR)

As the name implies, the SVR is Russia's service for conducting foreign intelligence activities. The organization descends directly from the KGB's First Chief Directorate. Its manpower is approximately 10,000 to 15,000, roughly a quarter of which is stationed abroad. According to the SVR's official website, it is divided into operational, analytical, and functional sub-elements. The main SVR operational directorates are reminiscent of several of Orlov's "lines of operation," and correspond with their Soviet-era predecessors. Chart 1 is adapted from the SVR's website.[131] Some of the directorate names and elements, such as Political Intelligence and Illegal Intelligence, are not listed on the chart but exist in the service.

Chart 1. Foreign Intelligence Service (SVR)


СЛУЖБА ВНЕШНЕЙ РАЗВЕДКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Zaslon
Director
Group of Consultants
Collegium
State Secretary
First Deputy SVR Director
Press Liaison
Director's Staff/Protocol
Assistant Director for Science
Assistant Director for Operations
Assistant Director for Staff
Assistant Director Material/Technical Logistics
NTR (S&T Intelligence)
Operational Depts.
Operations and Support
Analysis and Information
Operational Technology
Foreign CI
Information Systems
ER (Economic Intelligence)
SVR Academy

Sources: Organization chart created by author from multiple sources, including the SVR website, www.svr.gov.ru; government seal image from Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Russian_Foreign_Intelligence_Agency.png.

Directorate PR: Political Intelligence is the primary operational directorate within the SVR and is the direct descendant of an element with the same mission that existed in the KGB First Chief Directorate. Directorate PR is divided into geographically focused departments that manage political intelligence operations in SVR *rezidenturas* around the world. SVR *rezidenturas* are divided into "lines" within which officers specialize in a type of intelligence. Political intelligence officers abroad work in what the SVR calls Line PR sections. The operations of this directorate will be discussed in more detail in Chapter 4.

Directorate NTR: Scientific and Technical Intelligence is the direct descendant of the KGB-era Directorate T. It collects technology that Russia determines it needs to defend itself against foreign weapon systems and to advance Russia's own science and technology (S&T) developments. Directorate NTR manages S&T collection operations in SVR *rezidenturas* abroad under what is known in the SVR as Line X. This directorate will be discussed in more detail in Chapter 5.

Directorate ER: Economic Intelligence manages operations to collect intelligence about and to influence foreign economic systems, known as Line ER operations in SVR *rezidenturas* abroad. The operations of this directorate will also be discussed in more detail in Chapter 5.

Directorate S: Illegal Intelligence is divided into both geographic and functional departments. The latter include departments for selecting and training illegals, developing cover legends, and providing transportation and funding for illegals abroad. Directorate S is also responsible for the SVR Mobilization Department, which administers the SVR's participation in wartime environments. It manages Line N operations, related to the illegals program, in SVR *rezidenturas* abroad. The operations of this directorate will be discussed in more detail in Chapter 8.

Directorate KR: External Counterintelligence carries out infiltration of foreign intelligence and security services and exercises surveillance over Russian citizens living outside the country. It manages Line KR operations in SVR *rezidenturas* abroad, which are responsible for monitoring diplomats at overseas Russian government facilities.

Directorate MS: *Мероприятия Содействия* (Measures of Support) replaced what was formerly Service A under the KGB, which ran "active measures" operations. Directorate MS operations derive from those of other directorates, using intelligence collected across the agency to create influence operations that support Russia's foreign policy priorities. These operations will be discussed in more detail in Chapter 7.

SVR analytical directorates produce both strategic analysis for Russian decisionmakers and tactical analysis for other SVR directorates.

- **The Analysis and Information Directorate** and **Directorate I: Computer Service (Information and Dissemination)** analyze and distribute intelligence data and publish daily current events summaries for Russia's president.
- **Directorate R: Operational Planning and Analysis** evaluates SVR operations abroad.

Functional Directorates include:

- **Directorate OT: Operational and Technical Support** is the descendant of the KGB directorate of the same name. It provides equipment and technical personnel to support SVR operations.
- **Academy of Foreign Intelligence (AVR),** the SVR's training academy, is the descendant of the KGB's Red Banner Intelligence Academy and trains SVR personnel.
- Personnel, internal security, and staff, and logistical units.

A special operations element known as **Zaslon** is reportedly directly subordinate to the SVR director. Zaslon is responsible for protecting senior Russian embassy officials and other Russian government officials when they travel to dangerous locations. For example, Zaslon officers provided security when then-Russian Vice Prime Minister Dmitriy Rogozin traveled to Syria in 2014.[132] The element also conducts covert action missions. Little is publicly known about the group, but it reportedly was created in 1998 to replace special forces units that had been subordinate to the KGB First Chief Directorate during the Soviet era and moved to the Ministry of Security after the dissolution of the Soviet Union (for further information on covert action elements, see FSB Alfa and Vympel units below).[133]

As of 2021, the director of the SVR is **Sergey Yevgenyevich Naryshkin**, a career KGB officer whose chekist mindset and loyalty to Putin have propelled him into senior political positions. He joined the KGB in 1978, not long after Putin, and both worked in Leningrad at the same time. Naryshkin remained in the KGB up to the end of the Soviet era, operating under diplomatic cover in Belgium collecting S&T intelligence,[134] and he transitioned to the St. Petersburg city government soon after Putin did. When Putin moved to Moscow in the mid-1990s, Naryshkin remained in St. Petersburg, during which time he led foreign investment efforts for the St. Petersburg Oblast government.

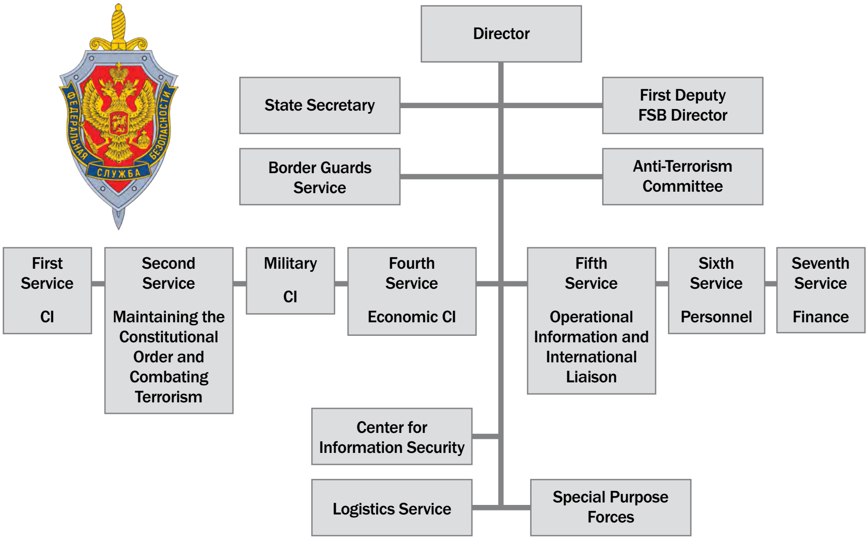
Naryshkin moved to Moscow in 2004, where his career has greatly benefitted from his proximity to Putin. At that time, Putin appointed him as an economic advisor in the Russian Presidential Administration, and he simultaneously served on the board of directors of Sovcomflot, a Russian shipping company that specializes in gas and oil tankers; Rosneft, Russia's oil giant; and the Russian television company, Channel One. From 2008 to 2011, Naryshkin was director of the Russian Presidential Administration during the Dmitriy Medvedev presidency. In 2009, Medvedev appointed Naryshkin to the Historical Truth Commission, which is tasked with protecting Russia's historical reputation. In December 2011, he was elected to the State Duma, serving as its chairman until 2016. He was in this position during Russia's covert operation to annex Crimea, and he consequently became the target of U.S. and European Union sanctions for submitting legislation to institutionalize that illegal Russian government action. Putin appointed his close associate Naryshkin to lead the SVR in 2016.

FEDERAL SECURITY SERVICE (FSB)

The FSB has inherited most of the KGB's historical functions and, thus, is a large organization. Much of its manpower is in the Border Guard Service, which was resubordinated from the FPS to the FSB in 2003.

The FSB is Russia's primary internal security organization, and thus it has the bulk of resources devoted to that mission. The FSB has several main operational services, which correspond directly to Soviet-era KGB directorates and carry out the FSB's primary functions (see Chart 2).

Chart 2. Federal Security Service (FSB)


ФЕДЕРАЛЬНАЯ
СЛУЖБА
БЕЗОПАСНОСТИ
Director
State Secretary
First Deputy FSB Director
Border Guards Service
Anti-Terrorism Committee
First Service CI
Second Service Maintaining the Constitutional Order and Combating Terrorism
Military CI
Fourth Service Economic CI
Fifth Service Operational Information and International Liaison
Sixth Service Personnel
Seventh Service Finance
Center for Information Security
Logistics Service
Special Purpose Forces

Sources: Organization chart created by author from multiple sources, including the FSB website, https://fsb.dossier.center//; *government seal image from Wikimedia Commons,* https://commons.wikimedia.org/wiki/File:Emblem_of_Federal_security_service.svg.

The **Counterintelligence Service** is the remnant of the KGB Second Chief Directorate and is one of the primary elements of the FSB today. Its mission is to thwart attempts by foreign intelligence services to operate inside Russia, including penetrating foreign diplomatic establishments, harassing foreign diplomats, and investigating Russians who come in contact with foreigners. These operations will be discussed in more detail in Chapter 3.

The element called the **Service for the Defense of the Constitutional Order and Fight Against Terrorism** combines counterterrorism and constitutional order into one element. This service is responsible for combating terrorism, extremism, and ethnically based organized criminal activities. It also conducts counterintelligence activities in the ministries of Health, Culture, and Education, in the religious sphere, and in noncommercial organizations. The same people who investigate terrorism also investigate internal instability created by dissent or protests. Consequently, oppositionists are often charged with violating extremism laws, which are linked to terrorism laws.

This element's name is eerily reminiscent of the Soviet era, when in 1989 the KGB Fifth Directorate was renamed Directorate Z, or the Directorate to Defend the Constitution. This directorate was responsible for internal security functions against the Soviet people, including combating political dissent, controlling religious activity, and monitoring dissident writers and artists, all of which the KGB described as "ideological subversion."[135] The resurrection of an element with a similar name and portfolio gives the appearance that the FSB has brought back a modernized version of the KGB Fifth Directorate, now combined with counterterrorism.

The **Military Counterintelligence Service** is the remnant of the KGB Third Chief Directorate and the descendant of OOs in the early Soviet era and the UKR SMERSH of World War II. It monitors the loyalty of military forces and conducts CI investigations and operations inside military units. The FSB also manages a similar element that monitors the loyalty of personnel in the Internal, Emergencies, and Justice ministries. A history of FSB military CI, written in 2004, indicates that the directorate retained its military spirit and work ethic after the dissolution of the Soviet Union, although it shrank in size and underwent some reorganization. It is unclear whether the downsizing has been reversed since then.[136]

The **Economic Security Service** is the remnant of what was once called the KGB 6th Directorate. It is directed toward economic crimes and is organized around the venues where crime might take place: industry, the transportation infrastructure, the banking system, etc. Chapter 5 will discuss the FSB's role in the economic realm.

The **Border Guard Service** was a directorate under the KGB during the Soviet era but was separated from the security service in 1993 to become an independent agency. However, in 2003, it was returned to the FSB structure, and today makes up the largest personnel element in the FSB.

The **Center for Information Security** (TsIB), also called Center 18, conducts both internal Internet monitoring directed at Russian citizens and foreign intelligence collection. One of the elements that the FSB inherited from the former FAPSI, the TsIB has been discussed in public infrequently, initially in relation to requests for information about Internet users. For example, the owner of the website Roem.ru received a request from a TsIB officer in 2011 asking for information about a subscriber, originating from the email address cybercrime@fsb.ru.[137] More recently, TsIB has gained notoriety for its overseas operations. In 2017, the U.S. Department of Justice indicted several TsIB officers for hacking into millions of Yahoo email accounts.[138] Media reports also connect TsIB with the attempted hacking of election systems in several states during the 2016 U.S. elections, which, when the attempts became public, led to arrests of TsIB officers in Russia for allegedly compromising the operation to the U.S. Government. The officers were charged with espionage on behalf of the United States.[139] The FSB also sponsors multiple advanced persistent threat computer-network actors, including one known in the West as Venomous Bear, aka Turla, which may be affiliated with TsIB.[140] TsIB reportedly operates in concert with an FSB SIGINT unit known as Center 16 in targeting Ukrainian government, law enforcement, and military entities.[141]

The FSB also inherited two **special purpose covert action elements** from the KGB, called Alfa and Vympel. The units were part of the KGB First Chief Directorate during the Soviet era and had a foreign covert action role.[142] When the SVR was created in 1991, they were transferred to an internal security function, necessitating their later replacement with Zaslon in the SVR. Alfa and Vympel are responsible for tracking and neutralizing terrorists or other threatening entities inside Russia. They have been deployed in the Chechen wars and during hostage situations in the North Caucasus, such as the Beslan school and Budennovsk hospital operations. Although they are described as domestic counterterrorism forces, these elements have reportedly recently resumed a foreign covert operations mission similar to their KGB predecessors. A 2020 Bellingcat investigation indicated that the assassin involved in the August 2019 murder of Georgian émigré and Chechen militant, Zelimkhan Khangoshvili, in Germany was associated with Vympel.[143] Alfa and Vympel may also have been behind the assassinations of other Chechen militant leaders outside Russia, such as in Turkey (see Chapter 7).

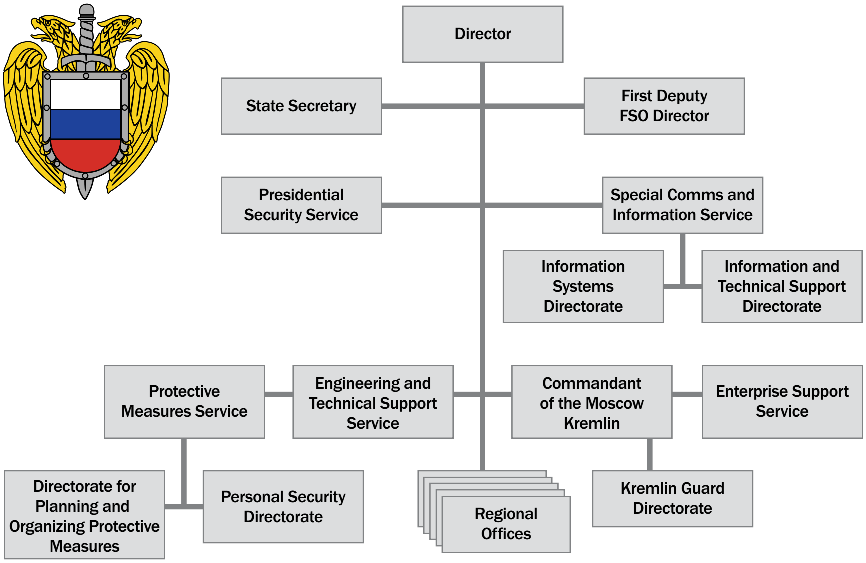
As of 2021, the director of the FSB is **Aleksandr Vasilyevich Bortnikov**. Like SVR Director Naryshkin, Bortnikov is a career state security officer, beginning in 1975. He also worked in Leningrad/St. Petersburg at the same time as Putin, and he remained in St. Petersburg until 2004, finishing his time there as chief of the St. Petersburg and Leningrad Oblast FSB office. Bortnikov moved to Moscow in 2004 to become director of the FSB's Economic Security Service, and he has served as FSB director since 2008. He holds the rank equivalent to a four-star general.

It is notable that both Naryshkin and Bortnikov, long-time Putin associates, were selected for positions close to Dmitriy Medvedev when he became president in 2008. Their regular association with Medvedev reinforced Putin's influence in Medvedev's administration.

FEDERAL PROTECTIVE SERVICE (FSO)

Another player with significant influence in Russian internal security is *Федеральная Служба Охраны* (Federal Protective Service, FSO). Its best-known role is to protect the Russian president and about 40 other senior government officials, including the prime minister, the chairmen of the Federation Council and State Duma, the chief of the Presidential Administration, the chairman of the Security Council, and the FSB director. The FSO is the descendant of several pieces of the former KGB: the Ninth Directorate, which was responsible for senior leader security; the 15th Directorate, which was responsible for protecting important government facilities; and parts of the Eighth Directorate, which secured Russian government communications. The FSO's current functions, as defined by the 2004 law under which it operates, fall into those same three categories: safeguarding senior leaders, providing security for protected facilities, and securing government communications, including special encrypted communications (see Chart 3).[144]

Chart 3. Federal Protective Service (FSO)


Director
State Secretary
First Deputy FSO Director
Presidential Security Service
Special Comms and Information Service
Information Systems Directorate
Information and Technical Support Directorate
Protective Measures Service
Engineering and Technical Support Service
Commandant of the Moscow Kremlin
Enterprise Support Service
Directorate for Planning and Organizing Protective Measures
Personal Security Directorate
Regional Offices
Kremlin Guard Directorate

Sources: Organization chart created by author from multiple sources, including the Russia Wikipedia website https://ru.wikipedia.org/wiki/*Федеральная_служба_охраны; government seal image from Wikimedia Commons,* https://commons.wikimedia.org/wiki/File:Great_emblem_of_the_Federal_Guard_Service.svg.

The FSO consists of the Presidential Security Service, the Directorate of Special Communications and Information (see Chapter 3 for information about FSO domestic sentiment analysis), protective security planning and organizational directorates, engineering and technical directorates, and housekeeping functions. The FSO also maintains offices in each of the federal regions around the country, which are responsible for the security of senior government officials there.[145]

As of 2021, the director of the FSO is **Colonel-General Dmitriy Viktorovich Kochnev**, who was appointed to that position in May 2016.

Kochnev has worked in the FSO since 2002 and, during the year before being named director, he served as the deputy director and chief of the Presidential Security Service. He has worked in Soviet/Russian state security organizations since 1982.[146]

NATIONAL GUARD

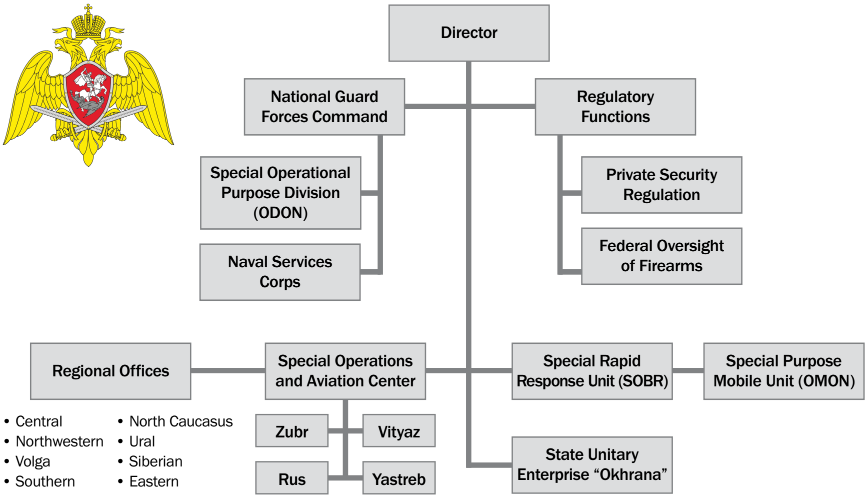
In 2016, Russia created a new security service called *Rosgvardiya* (National Guard of the Russian Federation), assembled mostly from pieces of the Ministry of Internal Affairs. Its purpose is to respond to what the Russian government calls "destabilization attempts," or what outside Russia would be called popular discontent. Its mandate includes suppressing protests both in the physical realm and the computer-based realm.[147] Some have questioned why, if Putin is so popular, he needed to create a security service directed at suppressing the Russian people. As the commander of the National Guard, Viktor Zolotov, spelled out in 2017, referring to anti-government protests:

> The protests are clearly systemic and have scenarios similar to those of color revolutions in other countries. The genuine goal of the fight against corruption is being substituted with general destabilization and chaos. Under the pretext of violations of rights and democratic freedoms in Russia, mass media outlets in the European Union, the United Kingdom, and the United States are constantly launching information attacks aimed at the political discrediting of the leadership of our country.[148]

Similarly, former FSB Director Nikolay Kovalev claimed that the creation of the National Guard "becomes especially topical amid the continued expansion of the North Atlantic alliance towards our borders and its heads openly state the intention to contain Russia. We register such calls ever more frequently."[149] In other words, Zolotov and Kovalev blame foreign powers for any manifestation of discontent within Russia. The National Guard was established with the same chekist mindset on which all other Russian intelligence and state security services are founded.

The National Guard consists of special police, rapid reaction, and counterterrorism units. Some of its missions overlap considerably with the FSB, although the primary purpose of the National Guard is to remain organizationally close to the president in case of internal disorder and dissent. The National Guard also maintains a strong presence in the North Caucasus, where it actively counters internal dissent (see Chart 4).

Chart 4. National Guard


Director
National Guard Forces Command
Regulatory Functions
Special Operational Purpose Division (ODON)
Naval Services Corps
Private Security Regulation
Federal Oversight of Firearms
Regional Offices
• Central
• Northwestern
• Volga
• Southern
• North Caucasus
• Ural
• Siberian
• Eastern
Special Operations and Aviation Center
Zubr
Vityaz
Rus
Yastreb
Special Rapid Response Unit (SOBR)
Special Purpose Mobile Unit (OMON)
State Unitary Enterprise "Okhrana"

Sources: Organization chart created by author from multiple sources, including the website of the National Guard of Russia, https://rosguard.gov.ru/; *government seal image from Wikimedia Commons,* https://commons.wikimedia.org/wiki/File:National_Guard_of_Russia.svg.

The chief of the National Guard, since its founding, is **Viktor Vasilyevich Zolotov**. He was a KGB Ninth Directorate officer from the 1970s, moving to the newly formed GUO in 1990 to serve on Boris Yeltsin's security detail. Zolotov has been a close associate of Vladimir Putin since at least the early 1990s when Zolotov served as the bodyguard for Anatoliy

Sobchak, the mayor of St. Petersburg, under whom Putin worked as deputy; Zolotov reportedly now serves as Putin's judo sparring partner.[150] Zolotov was a senior figure in the FSO from its founding in 1996 but moved to the MVD in 2013 to serve as commander of MVD internal troops. When those troops transitioned into the newly created National Guard in 2016, he became the new agency's first director.[151]

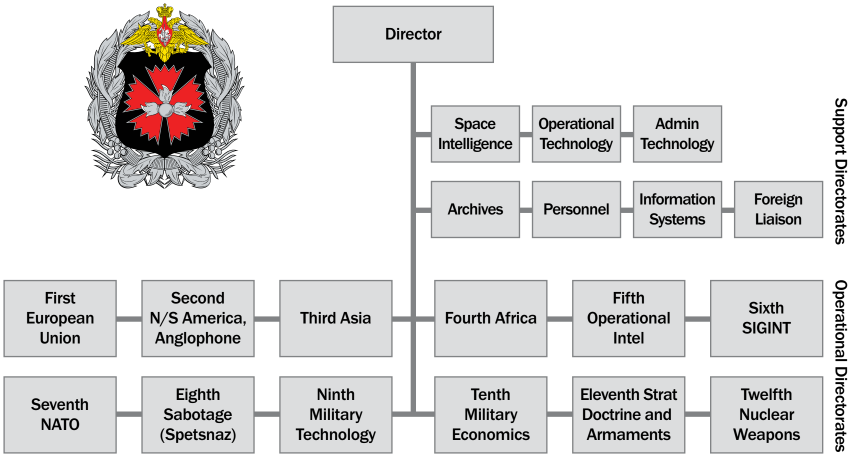
Comparing Security Personnel in Soviet Era to Today's Russia

Combining all of the agencies that have a security function in Russia, there are more security personnel per capita in Russia today than there were during the Soviet era. In 1991, there were approximately 490,000 KGB personnel in a country of 291 million people, which calculates as one state security employee for every 593 citizens. More recently, the FSB, SVR, and FSO combined have approximately 350,000 personnel in a country of 141 million, which calculates to one for every 402 citizens. Add to that the Russian National Guard, with its approximately 340,000 internal troops, and Russia today has nearly three times the number of people working in KGB successor organizations per capita than state security organizations had during the Soviet era.

MAIN DIRECTORATE OF THE GENERAL STAFF (GU)

The GU (until 2010, the GRU) is responsible for both intelligence collection to support military decisionmaking and covert operations to support foreign policy objectives, as it has since the founding of military intelligence in the Soviet era. Its organization—both geographically and functionally—reflects those two missions. The intelligence mission includes directorates that cover the European Union; North and South America, along with Anglophone countries; Asia; and Africa. Another directorate focuses on NATO specifically. Other directorates cover functional intelligence areas, including military technology, military economics, strategic doctrine and armaments, and nuclear weapons. A separate directorate houses SIGINT, which includes space-based and battlefield SIGINT platforms (see Chapter 9). Management of covert action is handled by another directorate, called the Diversionary, or Sabotage, Directorate, which houses *Spetsnaz* (GRU Special Purpose forces) (see Chart 5).

Chart 5. Main Directorate of the General Staff (GU)



Sources: Organization chart created by author from multiple sources, including the Russia Wikipedia website, Главное управление Генерального штаба — Википедия (wikipedia.org)*; government seal image from Wikimedia Commons,* https://commons.wikimedia.org/wiki/File:Emblem_of_the_GRU.svg.

As of 2021, the GU director is **Igor Olegovich Kostyukov**, the first Navy admiral to lead Russian military intelligence. He was appointed at a turbulent time in the service's history, in the midst of multiple public exposures of GU tradecraft and operations since 2016, primarily focused on the covert action side of the GU's mission. Kostyukov's two predecessors both died suddenly while in office, although there is no apparent foundation for rumors of foul play in either death. The official Russian version of GU Director Igor Dmitriyevich Sergun's death in January 2016 states that he died of a heart attack in Moscow. He was replaced by Igor Valentinovich

Korobov, who died after less than three years as GU director. In 2016 and 2017, all three officers were recognized with the Hero of the Russian Federation award, with Sergun's award being posthumous.

RIVALRY AMONG SERVICES

The various Russian intelligence and state security services have a tradition of rivalry, partially due to intentional overlaps in their missions. The KGB's First, Second, and Third Chief Directorates (now the SVR, the FSB's Counterintelligence Service, and the FSB's Military Counterintelligence Service, respectively) frequently fought for power, personnel, and resources within the Soviet system. The First Chief Directorate viewed itself as more sophisticated than and superior to its internal sister organizations. The First Chief Directorate also clashed with the GRU, as manifested when the Soviet government experimented with the Committee of Information in the late 1940s and early 1950s. The GRU refused to cooperate with civilian intelligence and removed itself from the organization after only a year. The GRU viewed the KGB and its predecessors as "chekist" organizations that were more aligned with purges and internal oppression than with intelligence work.

The rivalries continue today, with organizations' missions overlapping in such areas as counterterrorism, covert action, and operations in the Near Abroad. When Russian intelligence organizations conducted computer intrusions into the Democratic National Committee in the United States in 2016, both the GRU and probably the FSB ran parallel, uncoordinated operations in the same servers, apparently unaware of each other's operations.[152]

Rumors often float in Moscow about major reorganizations of intelligence and security services, some of which probably originate from the services' rivalry. In 2016, a Russian newspaper reported a rumor that the Russian government planned to create a "Ministry of State Security" similar to what had existed during the Soviet era. The rumored ministry would be based on the FSB, with the FSO and SVR rejoining it, nearly mirroring the KGB. The rumors came soon after the creation of the National Guard, when other law enforcement functions that had been housed in independent agencies, like the Federal Tax Police, were attached to the MVD.[153] Just six days after the original report, the same newspaper walked back the story and called it a "rumor;"[154] no such reorganization occurred. The rumors may have been intentionally leaked in the ongoing battle between intelligence and security services, either by the SVR to ward off FSB overreach by equating the FSB with feared Soviet-era organizations, or by the FSB to gauge public reaction to a possible power grab. Either way, the rumors quickly faded, and nothing came of them.

PUBLIC PERCEPTIONS

The public perception of state security can at times be negative. State security is not sacrosanct. A 2019 op-ed in a Russian newspaper discussing a mandate for Russian communications companies to provide encryption keys to the FSB stated, "It is obvious that the fact of providing keys works against a company. The reputation that our *siloviki* (security services) have is such that any structure that cooperates with them loses in the eyes of society. Resistance to their pressure, on the other hand, strengthens a company's position in public opinion."[155] Being seen as bending to state security demands can be bad for business.

Recent activities—ranging from ill-advised to illegal—by FSB officers have tainted the service in the public eye. In 2016, graduates of the FSB academy produced a film of themselves driving around Moscow in formation in expensive Mercedes Benz SUVs, waving and cheering themselves. It was an embarrassing lapse of security for recently graduated officers. Heads rolled in the FSB, and the graduates themselves were threatened with banishment to minor offices in the provinces.[156] Publicly, the event gave the impression of a young cadre of unruly, self-centered officers that contrasts with the patriotic image that the FSB tries to portray.[157]

More recently, FSB officers have been arrested on a variety of corruption charges. In spring 2019, an FSB colonel in the counter-corruption directorate was arrested with several colleagues for taking bribes. In July 2019, FSB officers were arrested and accused of robbing a bank and extorting money from a businessman. About the same time, the special assistant to the Presidential Special Envoy to the Urals and a member of the Security Council was arrested for high treason for communications with Poland. State security officers are under greater pressure today than they have been for a long time—at least since the FSB's involvement in botched counterterrorism operations in the early 2000s. Reports of the FSB's involvement in the attempted assassination of Aleksey Navalny in 2020 and Navalny's subsequent ability to trick a reported FSB officer into discussing the operation have further embarrassed the service.[158]

CONCLUSION: HISTORICALLY GROUNDED IN THE SOVIET ERA

Russian intelligence and state security organizations today are firmly founded on their Soviet predecessors, both in structure and in mindset. They continue to manifest historical chekist attitudes that see any internal dissatisfaction with the regime as being caused by foreign infiltrations. However, post-Soviet services today, including the SVR, FSB, FSO, GRU, and National Guard, are more prevalent and larger per capita even than during the Soviet era. Much of that manpower is directed internally at gauging, monitoring, suppressing, and demonizing internal dissent, which will be the topic of Chapter 3.

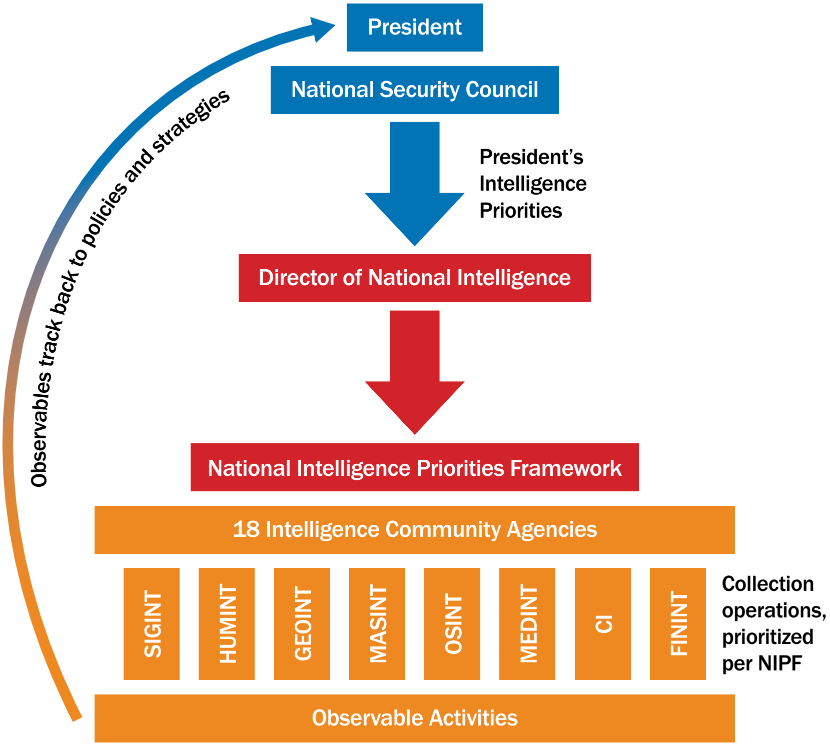
SECTION II

WHY

Analyzing National Security Priorities. A country directs its intelligence capabilities toward its highest priority concerns, and thus, by looking at where a country applies those capabilities, we can infer its priorities. In other words, if we look at what a country's intelligence system tasks its assets to collect and what placement and access it seeks in its sources, we can begin to develop an image of that country's priorities. Add to that analysis how the system is organized and on what targets it places the preponderance of its resources and the types of liaison relationships it develops and why, and that image becomes even clearer.

For example, over its history, the United States has developed a particular model for the policymaker-intelligence relationship, based on an intelligence system within a democratic society that recognizes the legitimacy of an elected leader and accepts guidance based upon legally defined relationships (see Figure 5). In this model, the President and National Security Council formally and informally articulate their intelligence priorities, in which they identify the national security issues that are at the forefront of their attention and the areas where they need intelligence to inform policy. These priorities shift and evolve at irregular intervals, based on geopolitical events and domestic politics. The National Security Council conveys the President's priorities to the Director of National Intelligence, whose staff translates them into the National Intelligence Priorities Framework (NIPF). U.S. intelligence agencies take their collection, analysis, and dissemination priority guidance from the NIPF by breaking it down into the requirements on which they focus their efforts.

Figure 5. U.S. Intelligence Priority Structure


President
National Security Council
President's Intelligence Priorities
Director of National Intelligence
National Intelligence Priorities Framework
18 Intelligence Community Agencies
SIGINT
HUMINT
GEOINT
MASINT
OSINT
MEDINT
CI
FININT
Collection operations, prioritized per NIPF
Observable Activities
Observables track back to policies and strategies

The phrase "intelligence system" describes the entirety of a country's intelligence and security resources, since most governments have more than one organization to fulfill these tasks. In the United States, we call the system a "community," consisting of 18 agencies and numerous sub-elements, ideally all working in unison to fulfill decisionmakers' needs. Russia, on the other hand, has four main intelligence and security services (FSB, SVR, GRU, and FSO), along with other supporting organizations (Ministry of Interior, National Guard, Investigative Committee, etc.). To understand the entirety of national security priorities, we would need to look at the activities of all of these organizations together as a system. Although the U.S. and Russian systems differ significantly in form, each serves its respective decisionmakers' end goals. Even where agency-specific agendas differ or agencies specialize in certain aspects of the bigger intelligence picture, the aggregate end product informs the deliberations of the state's decisionmakers.

Orlov's Lines of Operation. This section looks at how those priorities manifest themselves in the Russian intelligence system. It is organized around Alexander Orlov's eight "lines of operation," as the former Soviet intelligence officer described in his 1963 book, *Handbook of Intelligence and Guerrilla Warfare.*[159] Orlov's lines focused on external activities; however, based on the resources applied and using a modified version of Orlov's construct, internal security would appear to be Russia's highest priority. Among external operations, political intelligence collection is clearly a priority for Russia, based on the numerous reported Russian intelligence activities directed against political targets. Other priorities include economic and S&T intelligence and military intelligence, both of which protect Russia from what it perceives to be a threatening world bent on destroying it. Informed by the intelligence that these disciplines collect, Russian leaders have at their disposal a spectrum of action options, from public statements in the information realm to covert activities in the military realm. Intelligence and state security services also are responsible for executing some of these options. Although covert activities such as political manipulation and assassinations are prominent in the media, they need to be analyzed in the context of other priorities placed on Russian intelligence and state security services. This section will analyze those major priority areas.

Orlov's first line of operation was what he called "diplomatic intelligence," or what Russian intelligence services today call political intelligence. This means the collection of intelligence to support the foreign policy decisionmaking of the Russian leadership. For the KGB during the Cold War and the SVR today, political intelligence has always been a major effort, and the largest section in an SVR *rezidentura* is ***политическая разведка*** (political intelligence; Line PR). These operations will be discussed in Chapter 3. The second line of operation is the infiltration of foreign countries' security agencies and intelligence services. This line has both counterespionage and foreign intelligence purposes. While infiltrating a foreign intelligence service provides the obvious opportunity to identify recruited agents inside one's own government, foreign intelligence services also have access to classified information from across their government, including foreign policy and military plans, making them lucrative intelligence targets. Penetrating a foreign intelligence service could also yield information about encrypted means of communication, which can be exploited for further intelligence collection purposes. The role of infiltrating foreign intelligence and security services inside Russia today is fulfilled by the FSB, while that same function outside Russia is the responsibility of the SVR, which has an element dedicated to foreign counterintelligence. These will be discussed in Chapter 4.

The next two lines of operation are economic intelligence and what Orlov called "industrial intelligence." Economic intelligence is the information Russia requires to understand the economic levers that other countries are employing against Russia. It also encompasses efforts to uncover perceived foreign plots to damage Russia's economy. This is partially the SVR's responsibility, but the FSB, which has an economic counterintelligence mission, also plays a role. Orlov's industrial intelligence, which today is called science and technology (S&T) intelligence, seeks to collect foreign countries' latest scientific advances that Russia can use either to fuel its own technology development or to form the basis of countermeasures. In the latter category, the priority falls on foreign military technology to support Russian military planning. S&T intelligence is the responsibility of both the GRU, which particularly focuses on military technology, and the SVR. These will be discussed together in Chapter 5.

Orlov's fifth line of operation is military intelligence, which seeks information the Russian military will need to fight. This can run the spectrum from tactical information about military units and equipment to information about the strategic targets Russia would need to strike and neutralize to be victorious in a future war. Russia's military intelligence service, the GRU, is predominant in this area of intelligence collection. However, both the SVR and FSB also participate in collecting intelligence about foreign military capabilities and intentions. Military intelligence will be discussed in Chapter 6.

Orlov's last three lines of operation are misinformation, influencing foreign governments' decisions, and sabotage and guerrilla warfare. Rather than intelligence collection missions, these are policy execution missions assigned to Russia's clandestine services. Misinformation has become the most well-known of these through widely publicized Russian efforts, from meddling in foreign elections to manipulating foreign investigations of aggressive Russian actions abroad. Formerly labeled "active measures," this Cold War-era term has been replaced in the Russian system by the phrase "*мероприятия содействия*" ("measures of support"). Influencing foreign governments' decisions can take the form of recruiting assets with access to policymaking circles who subtly use their proximity to sway decisions toward Russia's favor. Sabotage and guerrilla warfare have factored into Soviet/Russian intelligence activities since the Bolshevik revolution. As noted in Chapter 1, the Russian word *разведка*, which is usually translated in English as intelligence, expands beyond collecting information to employing covert operations against an enemy force and includes activities from supporting foreign revolutions to targeting an enemy's critical and military infrastructure during wartime. These three lines of operation benefit from the intelligence collected by the other lines and represent clandestine and covert tools that Russia can use to advance its own political, military, and economic goals. Covert operations in their various forms will be discussed in Chapter 7.

This section looks at the Russian intelligence system and the primary categories of effort the Russian government employs that system to fulfill. From that structure, along with the resources dedicated to those categories, we can derive Russia's overall national security priorities.

CHAPTER 3

INTERNAL SECURITY AND COUNTERINTELLIGENCE

Russian state security begins with securing the internal political environment. By far the largest portion of Russia's intelligence and security resources are directed at countering internal threats. Counterintelligence in its Russian definition includes working against foreign intelligence services, as is typical of other countries. However, Russian CI extends further to securing the ruling regime from any political threats, regardless of their origin. Protecting the regime is the primary purpose of Russia's intelligence and state security services, particularly the FSB, FSO, and National Guard, and the SVR outside Russia.

Internal security is intended to counter potential threats from several directions:

- Foreign intelligence services operating inside Russia.
- Terrorism.
- Dissent and anti-regime activities.
- Economic crimes.

All of these categories are combined together in the view of Russia's internal security apparatus. This chapter will be organized around the first three of these directions, while the fourth, economic crimes, will be described in Chapter 5.

COUNTERING FOREIGN INTELLIGENCE SERVICES

Since at least 2012, Vladimir Putin has given an annual address at the FSB's Lubyanka Headquarters, where he has praised the service for its success in catching spies. In his speech, he has usually cited statistics about foreign intelligence-affiliated persons whom the FSB has neutralized in the

Table 2. Foreign Intelligence Operations Neutralized, per Putin

	Foreign Officers	Agents of Foreign Intelligence	Total
2012	34	181	**215**
2013	no data	no data	**?**
2014	>50	almost 300	**~350**
2015			**>400***
2016	53	386	**439**
2017	72	397	**469**
2018	129	465	**594**
2019	no data	no data	**?**
2020	72	423	**495**

**Putin gave only an approximate aggregate number in his 2016 speech covering 2015 statistics.*

Sources: “Заседание коллегии Федеральной службы безопасности” [“Conference of the Federal Security Service Collegium”], Kremlin.ru, February 14, 2013, http://kremlin.ru/events/president/news/17516*; “ФСБ сюсюкать не будет: На все угрозы национальной безопасности Путин пообещал адекватный ответ” [“The FSB Is Not Lisping: Putin Promised an Active Response to All Threats to National Security”], Lenta.ru, March 26, 2015; “Заседание коллегии Федеральной службы безопасности” [“Conference of the Federal Security Service Collegium”], Sosluzhivtsi.ru, February 26, 2016,* https://sosluzhivtsi.ru/public/politika/1977-zasedanie-kollegii-fsb/*; “Заседание коллегии Федеральной службы безопасности” [“Conference of the Federal Security Service Collegium”], Kremlin.ru, February 16, 2017,* http://kremlin.ru/events/president/news/53883*; “Заседание коллегии Федеральной службы безопасности” [“Conference of the Federal Security Service Collegium”], Kremlin.ru, March 5, 2018,* http://kremlin.ru/events/president/news/56977*; “Заседание коллегии Федеральной службы безопасности” [“Conference of the Federal Security Service Collegium”], Kremlin.ru, March 6, 2019,* http://kremlin.ru/events/president/news/59978*; “Заседание коллегии ФСБ” [“Conference of the FSB Collegium”], Kremlin.ru, February 20, 2020,* http://kremlin.ru/events/president/news/62834*; “Заседание коллегии ФСБ России” [“Conference of the FSB Collegium of Russia”], Kremlin.ru, February 24, 2021,* http://www.kremlin.ru/events/president/news/65068*.*

previous year, including foreign intelligence service staff personnel and their agents (see Table 2). Up to 2020, the numbers had grown each year, and by 2018 were astronomical: nearly 600 people. In 2020 the numbers dropped for the first time since 2012, according to Putin's 2021 speech, only because of the "demands of the current epidemiological situation."[160] Putin has cited no data to support the numbers and has said nothing about the countries involved or suspects' names. For unknown reasons, he did not cite concrete 2019 statistics in his 2020 address; however, he did stress that counterintelligence remains a crucial part of FSB's activities and "figures show that the activity level of foreign special services in our country is not declining."[161]

Putin makes such outlandish assertions to substantiate Russian claims that Russia is increasingly under siege by adversarial foreign powers. The numbers send a message to the Russian people to be on alert for foreign spies everywhere and thus justify the implementation of strict internal security measures, including those that restrict the rights of Russians domestically. Furthermore, the numbers probably represent retaliation for CI activities against Russia abroad. Russia's 2018 arrest count undoubtedly includes an American named Paul Whelan, who was arrested for espionage on December 28,[162] just 15 days after Mariya Butina, accused of acting as an unregistered foreign agent for Russia, pleaded guilty to conducting a clandestine political influence operation in the United States.[163]

Putin's citation of espionage statistics is reminiscent of reports that his idol, former KGB Director Yuriy Andropov, provided to the Soviet Communist Party leadership. In 1968, for example, Andropov gave an account of arrests that had occurred during 1967, which stated that the KGB "brought to justice 738 persons, 263 for particularly dangerous state crimes, and 475 persons for other state crimes."[164] Those convicted for criminal offenses included:

- 3 who carried out diversion operations.
- 121 traitors and war criminals from the German-Fascist occupation.
- 34 indicted for treason to the Motherland and for treasonous plotting.

- 96 persons for anti-Soviet agitation and propaganda.
- 221 persons for illegal crossing of state borders.
- 100 persons for embezzlement of state and public property in large amounts and for corruption.
- 148 for illegal smuggling of goods and for violations of currency operations rules.
- 1 foreigner and 1 Soviet citizen who were arrested for espionage.

Putin appears to have resurrected this Andropov-era accounting, even approaching the number of arrests Andropov reported in 1968. Although not specified, Putin's aggregated numbers probably combine crimes such as treason, anti-Russian agitation and propaganda, and espionage, just as Andropov's numbers did.

Embassy Operations

It is axiomatic that an intelligence or counterintelligence service is more capable on its home territory than in places it does not control. Consequently, Russian CI operations inside Russia are more capable than operations elsewhere. This reality applies to Russian operations targeting foreign diplomatic establishments inside Russia.

Defectors throughout Soviet history have provided consistent reports of active infiltrations of foreign embassies in Moscow. Aleksandr Zhigunov, an NKVD counterintelligence officer captured by German forces during World War II, told his German interrogators about Soviet operations against embassies in Moscow, specifically noting targeting of the German and Hungarian embassies.[165] Zhigunov also discussed the September 1939 visit by Turkish Foreign Minister Sukru Saracoğlu to Moscow to negotiate a mutual assistance treaty, noting that Saracoğlu was under NKVD observation during his entire visit, particularly during a long car ride he took with a British embassy official through the streets of Moscow.[166] KGB defector Yuriy Rastvorov reported participating in operations soon after World War II to recruit sources among Japanese diplomats, particularly using women as bait to lure targets into compromising situations.[167] Afanasiy Shorokhov (aka Vladimir Petrov) reported an almost identical operation also targeting a Japanese diplomat.[168] The first U.S. individual to defect to the Soviet Union during the Cold War—James MacMillan, a cipher clerk at the U.S. embassy in Moscow—was recruited by the MGB in 1948 with the help of a Russian woman.[169]

In addition to human targeting, the KGB extensively used technical means to penetrate foreign embassies in Moscow, from miniature microphones embedded in furniture or walls to directing microwaves, infrared light, or lasers at an embassy.[170] In October 1963, former KGB officer Aleksandr Cherepanov passed a package of documents to an American tourist in Moscow and asked him to give it to the U.S. Embassy. The documents contained details of KGB counterintelligence methods, personnel, and technical devices employed in operations.[171] Rather than accepting the documents and following up with Cherepanov, the U.S. Embassy—against the CIA's wishes—returned them to the Soviet government, although the CIA did take the opportunity to photograph them. Cherepanov was soon arrested, and he was executed in April 1964.[172] Also in 1964, Yuriy Nosenko, another KGB officer, defected and provided additional details of Russian targeting of the U.S. Embassy in Moscow. Nosenko revealed the KGB Second Chief Directorate was targeting hundreds of foreigners, including diplomats and journalists in Moscow and visitors to the Soviet Union, for counterintelligence purposes.[173]

Today, the FSB is the primary Russian organization responsible for penetrating foreign diplomatic establishments in Russia. The FSB still uses both human and technical means for that purpose. For example, FSB officers coerced a Russian citizen to pass information on the UK's visa application system. The individual worked for a company TLSContact that provides computer network services for consulates, and he provided computer assistance to the British consulate in Russia until he fled in 2016. The FSB reportedly attempted to use the Russian individual to explore options for clandestinely obtaining UK visas for two Russian travelers, who may have included the GRU officers responsible for the attempted assassination of Sergey Skripal in 2018.[174] The FSB reportedly also recruited a Russian woman who served as a liaison between the U.S. Secret Service office in Moscow and Russia's law enforcement and intelligence agencies. The woman had access to a U.S. Embassy email system until she was fired from her employment in 2017.[175]

Computers at the Armenian embassy in Moscow were reportedly broken into in 2020[176]—an intrusion probably led by an FSB computer operations unit. A similar incident had been reported at the EU delegation in Moscow in 2017.[177] An unspecified European embassy in Moscow was among the targets of a spearphishing campaign detected in 2018 that involved emails masquerading as messages from Janes, the British defense journalism company, and targeting ministries of foreign affairs in North America and Europe.[178] Such incidents probably occur more often, but they are not reported because they either go undetected or the victims choose not to discuss their vulnerabilities publicly.

Russian attempts to penetrate foreign embassies can benefit both intelligence and counterintelligence missions. Intelligence purposes may include collecting personal information about individual employees that a Russian intelligence service could use for HUMINT recruitment efforts or, as noted above, to obtain visas for clandestine travelers. Such operations also provide political information, plans, and priorities of the embassy staff, as well as potential access to cipher and encryption information to use in future SIGINT collection operations. Counterintelligence purposes include identifying foreign intelligence personnel posted to Russia under diplomatic cover. Embassy penetrations can also identify connections between foreign embassies and oppositionists inside Russia—an important target for Russian internal security operations. More broadly, they can inhibit embassy operations by preventing both clean diplomats and intelligence officers under diplomatic cover from fulfilling their mission.

One method the FSB uses to inhibit embassy operations is harassment of U.S. and other countries' diplomats in Russia, which has increased dramatically since 2014. Harassment has involved arbitrary police stops, physical assault, break-ins into diplomats' homes, and broadcasting their personal details on state TV channels, thereby placing them at risk of public harassment.[179] The FSB may employ diplomatic harassment for several reasons: as a tool to retaliate for U.S. counterintelligence or law enforcement operations directed at Russian diplomats, to identify diplomatically covered intelligence officers, to provoke a response that can be used against the United States in propaganda messaging, or simply to create stress among the diplomatic staff, thereby limiting their effectiveness. In general, the FSB's harassment of foreign diplomats is a counterintelligence method that the Russian government uses to reduce the overall effectiveness of foreign intelligence operations in Russia.

COUNTERTERRORISM

Russia's second leading internal security mission is counterterrorism. Russia has experienced significant terrorist attacks on its soil (see Figure 6). Countering terrorism is the primary mission of what is now called the FSB's Service for the Defense of Constitutional Order and Fight Against Terrorism. The Russian National Guard also has a counterterrorism function, and its inheritance of quick reaction units from the MVD in 2016 has created an overlap between the FSB and National Guard missions. Additionally, both the SVR and GRU have responsibilities for collecting intelligence about terrorism that threatens Russia, and the GRU *Spetsnaz* forces are trained to conduct counterterrorism operations. The Russian government claims success in countering terrorism, and it proudly proclaimed in April 2009 that counterterrorism operations in Chechnya were complete.[180] Putin holds up this stated success as a major accomplishment for his legacy, and it is one reason domestic support for Putin is high. However, major terrorist events in Russia did not end with the declaration of victory in Chechnya, and high-profile attacks have occurred since then in Moscow, St. Petersburg, and other Russian cities. In February 2021, Putin declared that 72 "terrorist crimes" had been thwarted in 2020, up from 57 in 2019, and that "in December last year, the last organized bandit group that was committing crimes on the territory of the Chechen Republic and Ingushetia was destroyed."[181]

Figure 6. Major Terrorist Attacks in Russia Since the Dissolution of the Soviet Union

Date	Description
June 1995	During the first Chechen war, Chechen fighters stormed a hospital in Budennovsk near the border with Russia, taking many civilians hostage (some estimates say as many as 2,000 people) and threatening to kill them unless the war ended. Russian forces' attempts to raid the hospital failed. More than 100 people were killed before an agreement was reached, and the militants were allowed to return to Chechnya.
January 1996	Chechen fighters took hundreds hostage in a hospital in Kizlyar, Dagestan, and moved them by bus to Pervomayskoye on the Chechen border. Most rebels escaped, but many hostages were killed during a rescue attempt.
September 1999	Bombings of apartment buildings killed almost 300 people in Moscow, Buynaksk, and Volgodonsk. The attacks were blamed on Chechen separatists and eventually led to the second Chechen war, but some conspiracy theories link Russia's intelligence services to the attacks.
October 2002	Dozens of Chechen militants seized the Dubrovka Theater in Moscow, taking 700 people hostage. Russian security forces attempted to enter the theater and pumped a strong narcotic gas into the building to sedate the attackers. Most of the casualties occurred in the raid, which happened on the third day of the crisis. Ultimately, 41 Chechen militants and 129 hostages were killed, most of them succumbing to the gas.
December 2002	A suicide truck bomb destroyed the headquarters of Chechnya's Moscow-backed government in Grozny, Chechnya. The attack left 72 people dead.
August 2003	Chechen militants killed 50 in a suicide bombing using a truck rigged with explosives and driven into a military hospital in Mozdok, North Ossetia.

Date	Description
December 2003	An explosion killed 46 people and injured an additional 146 near Yessentuki station in the Stavropol Krai.
February 2004	A suicide bomber hit the Moscow subway during rush hour, killing 41 people and wounding more than 100. A little-known Chechen group later claimed responsibility for the attack.
May 2004	A suicide attack at a stadium in Grozny killed 24 people. Among those killed was Akhmad Kadyrov, the Moscow-backed Chechen president and father of Chechen leader, Ramzan Kadyrov.
June 2004	Chechen militants stormed the interior ministry building in Nazran, Ingushetia, resulting in the deaths of at least 92 people, including acting regional Interior Minister Abukar Kostoyev.
August 2004	Two suicide attacks targeted flights from Moscow's Domodedovo airport. All 90 passengers on the flights were killed. The two female attackers were later found to have bribed an airline agent with 1,000 rubles (about $34 at the time) to board the planes. Just days later, a suicide bomber killed 10 people on the Moscow subway.
September 2004	Chechen rebels assaulted a children's school in the southern Russian city of Beslan, taking over 1,000 hostages. Those killed throughout the seizure and subsequent attack by Russian forces and local armed vigilante groups numbered more than 331, half of them children.
October 2005	Islamist militants launched attacks on police and government buildings in the city of Nalchik, Republic of Kabardino-Balkaria, in the North Caucasus. A large group of attackers targeted buildings housing the Russian security forces, killing more than 100 people, including civilians.
August 2009	A suicide bomber killed 20 people and injured 138 more after driving his truck, packed with explosives, into a police station in Nazran, Ingushetia.

Date	Description
November 2009	A suicide bomb exploded on the high-speed rail link from Moscow to St. Petersburg, killing 28 people and injuring 130. Ten men were imprisoned for their role in the attack, nine of whom were from the same family in Ingushetia. A second explosion occurred as investigators were searching the wreckage. The Caucasus Emirate movement was reported to have ordered the attack.
March 2010	Two female suicide bombers on the Moscow subway killed more than 40 people. One of the stations targeted, the Lubyanka Station, is near FSB headquarters.
January 2011	A suicide bombing at Moscow's Domodedovo airport killed 37 people and wounded 172. Doku Umarov of the Caucasus Emirate movement claimed responsibility for the attack.
August 2012	A suicide bomber attacked the funeral of a police officer fatally shot a day earlier in Russia's North Caucasus region, killing 7 people and injuring 10 in mourning.
October 2013	A female suicide bomber from Dagestan blew up a passenger bus in Volgograd, killing 6 people and wounding more than 30 others.
December 2013	Two suicide bombings a day apart targeted the public transport system in the city of Volgograd. A total of 34 people were killed in the attacks on a train station and a trolley bus, including the perpetrators. The bombings occurred weeks before the start of the 2014 Winter Olympics, being held about 400 miles away in the Russian Black Sea resort of Sochi.
October 2015	A charter jet taking Russian vacationers home to St. Petersburg from an Egyptian beach resort town crashed in a remote part of Egypt's Sinai Peninsula, killing all 224 passengers and crew members on board. Russian authorities concluded that a homemade bomb smuggled onto the jet detonated 23 minutes after it took off from Sharm el-Sheikh, the popular Red Sea resort town. Terrorists tied to the Islamic State claimed responsibility for the attack.

Date	Description
December 2016	A Russian flight traveling to Syria crashed into the Black Sea near Sochi, killing all 92 on board. A number of passengers were members of the Red Army choir scheduled to perform a New Year’s concert in Syria. Although authorities found no signs of an explosive, a terror motive was not ruled out.
April 2017	Two explosions killed at least 10 people and injured dozens more in a busy metro station in St. Petersburg.
December 2017	President Putin called President Trump to thank him for CIA-provided information that helped prevent an Islamic State attack in St. Petersburg. The attackers planned to strike crowded sites, including the Kazan Cathedral.
December 2017	A bomb exploded in a St. Petersburg supermarket, injuring 13 people. The bomb was hidden inside a rucksack in a locker where shoppers leave their belongings. The person who left the rucksack was described as being of “non-Slavic appearance.”
December 2019	President Putin thanked President Trump for U.S. intelligence that led to the FSB arresting two Russian nationals in St. Petersburg who were planning attacks on New Year’s Eve.

Sources: Figure created by author from multiple sources, including Adam Taylor, “The Recent History of Terrorist Attacks in Russia,” Washington Post*, April 3, 2017,* https://www.washingtonpost.com/news/worldviews/wp/2017/04/03/the-recent-history-of-terrorist-attacks-in-russia/*; David Filipov, “Putin Thanks Trump for CIA Intel that Foiled a Planned Terrorist Attack in Russia,”* Washington Post*, December 17, 2017,* https://www.washingtonpost.com/world/putin-thanks-trump-for-cia-intel-that-foiled-a-planned-terrorist-attack-in-russia-the-kremlin-says/2017/12/17/f4274600-e349-11e7-9ec2-518810e7d44d_story.html*; Isabelle Khurshudyan, “Putin Thanks Trump for Information That He Says Helped Foil a Planned Terrorist Attack in St. Petersburg,”* Washington Post*, December 30, 2019,* https://www.washingtonpost.com/world/putin-thanks-trump-for-information-that-helped-foil-a-planned-terrorist-attack-in-st-petersburg/2019/12/30/9788ee34-2b32-11ea-bffe-020c88b3f120_story.html*.*

When terrorist attacks occurred in the United States in September 2001, Russia was quick to offer its help. The Russian government claimed that it had been fighting terrorists for years and hoped that the new U.S. emphasis on terrorism would lead the United States to see things Russia’s way. However, Russia's definition of terrorism made cooperation difficult. Russia views terrorism broadly as a political threat to the Russian regime, and any violent act that harms Russia's influence or prestige around the world is terrorism; this interpretation can include anything from Islamist extremism to protests against the Russian government's handling of elections. In contrast, the United States defines terrorism as the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims. Russia's definition is internalized, while the U.S. definition is global.

Based on Russia's broad definition and its national experience with terrorism, the 2016 Russian Foreign Policy Concept of the Russian Federation includes strong language about the need to counter terrorism around the world. But, in addition to countering violent extremism, Russia's counterterrorism message carries a veiled criticism of U.S. policy: "The ideological values and prescriptions imposed from outside these countries [in the Middle East and North Africa] in an attempt to modernize their political systems have exacerbated the negative response of their societies to current challenges."[182] As the policy document goes on to say, the Russian Federation "categorically opposes any reliance by States on terrorist organizations in pursuit of political, ideological or other aims," and "advocates consolidating the UN-led collective efforts to defeat foreign terrorist fighters by blocking all forms of material support available to terrorist organizations."[183] Some of this language sounds familiar to a Western ear, and the Russian and U.S. definitions of terrorism have occasionally aligned, such as when the United States provided information to the Russian government that led to the neutralization of terrorist operations in St. Petersburg, Russia, in 2017 and 2019.[184] However, often it does not. Russia does not view groups affiliated with Iran as terrorists, while it does see U.S.-supported groups that oppose Syrian President Bashar al-Assad as terrorists. Russia viewed its two wars in Chechnya in the 1990s and early 2000s as wars against terrorism, while many in the West viewed them as civil wars in which the Russian government's brutal methods caused as much harm as good.[185]

The chekist mindset under which Russian counterterrorist agencies operate, which always sees foreign ties to domestic threats, also applies to terrorism. Putin and other government leaders espouse the narrative that any terrorist action inside Russia has been sponsored from abroad—to include foreign powers, especially the United States. After a car-bomb attack in 2009, then-interior minister of Dagestan, Ali Magomedov, is reported to have said, "Certainly, what is happening now is being exacerbated from outside, beyond the Russian borders. There can be no other explanation. Dagestani people do not need to kill one another."[186] Speaking to an SVR audience in 2017, SVR Director Sergey Naryshkin asserted, "You are well aware of the challenges that Russia faces. They include attempts to restrain our development, to impose confrontation, to destabilize the regions near Russia's borders, including by using terrorist and extremist groups as a weapon. It is no secret that some of these are carefully fostered, and even received direct support from the special services of a number of countries."[187]

In an interview with producer Oliver Stone in 2015, Vladimir Putin was more to the point: "You don't have to be a great analyst to see the United States supported financially, provided information, supported them [Chechen terrorists] politically. They supported the separatists and terrorists in the North Caucasus."[188] As noted earlier, Putin gained prominence initially and was first elected president on the reputation he built for being tough on terrorism and crime. His reputation for toughness is a foundation for his current popularity and translates today into rhetoric that ties foreign powers, especially the United States, to Russia's domestic terrorism problem.

COUNTERING DISSENT AND ANTI-REGIME ACTIVITIES

The third leading internal security mission is to suppress dissent and domestic anti-regime activities (see Figure 7). This is the most publicly visible aspect of Russia's internal security functions. Suppressing dissent has been an important element of Soviet internal security since the foundation of Soviet rule, especially during Stalin's reign. Per Deryabin's saying, the "god of state security" shifted to counterintelligence after World War II,[189] although Russia's definition of CI primarily encompassed state security efforts to prevent foreign influences from infiltrating the Soviet population and thus to counter the potential that the Soviet people could embrace democratic ideas. The list of successes noted above that Yuriy Andropov reported to the Communist Party leadership in 1968 included acts such as anti-Soviet agitation and propaganda as a state security threat. As noted earlier, Andropov also established the KGB's Fifth Directorate in the late 1960s, which was responsible for countering "ideological subversion," meaning any dissident or religious activity.

From the beginning of Putin's tenure as president, he has steadily increased the internal security services' power to monitor dissent and prevent it from gaining strength inside Russia. Much of today's effort dates from Putin's 2012 reelection and the public opposition that was expressed to his running again for president. The year 2012 was a watershed for Russia's response to internal dissent. The previous year, Putin announced he would run for president after one term as prime minister, in what some called a "castling" move.[190] Many Russians saw this as an unconstitutional usurpation of power, since Putin had already served two terms as president from 2000 to 2008. Thousands demonstrated against his return to the presidency, chanting "For Honest Elections," although his reelection was a foregone conclusion.[191] From December 2011 to May 2012, Russian police arrested hundreds of anti-Putin protestors, led by two prominent oppositionists: Boris Nemtsov, who was assassinated in 2016, and Aleksey Navalny, who was the target of an assassination attempt in 2020.[192] Putin's new term as president emboldened him to crack down on dissent, and Russian security services since then have followed that political imperative.

The FSB has many law enforcement tools available to suppress internal dissent among Russian citizens: tax laws; laws against extremism/terrorism and organized crime, as well as money laundering and narcotics trafficking; and laws that forbid inciting hatred or public insult of an authorized representative connected with the fulfillment of his responsibilities (see Chapter 5 for more information on the use of economic counterintelligence measures to suppress dissent). In June 2012, the State Duma passed amendments allowing judges to treat a single-person protest as an unsanctioned assembly if they detect a "common intent and organization."[193] In 2016, the Russian government established another entity to quash internal dissent, the National Guard, which is responsible for enforcing anti-assembly laws and preventing protests from threatening the ruling regime. Since then, the National Guard has been involved in suppressing multiple protest events across Russia.

Figure 7. **Notable Protest Actions in Russia**

2008: Small anti-war demonstration in Moscow against Russian war in Georgia

2011–13: Demonstrations in Moscow to protest presidential elections

2014: Small anti-war demonstrations against the Russian annexation of Crimea

2017–18: Anti-corruption protests in multiple cities

2018: Demonstrations across Russia to protest pension reform

2019: Demonstrations in Moscow to protest the disqualification of candidates for Moscow city council elections

2020: Demonstrations in Khabarovsk to protest the mayor's arrest and Moscow's influence in the region

2021: Demonstrations across the country protesting the arrest of Aleksey Navalny

Russian state security services have broad authority to intercept and monitor domestic communications within Russia. Russian law enforcement and security services use "lawful intercept" authority, through which they can access communications at gateways and nodes, potentially giving them visibility into all computer traffic traversing Russia's communications system. The *Система Оперативно-Розыскных Мероприятий* (System for Operational Investigative Measures; SORM) was initially implemented in 1995 and has been updated several times. SORM requires Russian communication providers, including voice and Internet, to install devices on their networks that allow the FSB to track all electronic traffic. As Internet technology has advanced, SORM rules have adapted to keep up. Multiple investigative organizations inside Russia have access to SORM data, including most prominently the FSB and its sub-element, the Border Guard Service; Russia's Tax Police within the Ministry of Internal Affairs (MVD); the FSO and its sub-elements, the Kremlin Regiment and the Presidential Security Service; and Parliamentary security services. SORM also offers its communications-monitoring capabilities to former Soviet states, which often use Russia-based communications lines.

Russia's monitoring of its internal networks has increasingly tightened over the past several years. In 2016, under the pretext of countering terrorism, the Russian State Duma adopted the Yarovaya Law, named after its parliamentary sponsor, Irina Yarovaya. The Yarovaya Law requires telecommunications providers to store the content of voice calls, data, images, and text messages for six months and the metadata associated with them (e.g., time, location, sender, and recipients of a message) for three years. Online services such as messaging services, email, and social networks that use encrypted data are required to allow the FSB to access and read their encrypted communications.[194] Internet and telecommunications companies must disclose these communications and metadata and "all other information necessary" to authorities on request and without a court order.[195] This requirement was originally scheduled to take effect on July 1, 2018; however, the State Duma decided to postpone the start date until 2023 to allow companies time to install the extreme amount of data storage needed to fulfill it.

The FSB began enforcing a demand for telecommunications companies to provide encryption keys for traffic traversing their networks in 2017, but several companies have resisted. The chat service Telegram refused to provide encryption keys in 2017, as did the Internet service provider Yandex in 2019. After Telegram founder Pavel Durov refused, Russia's telecommunication watchdog organization, Roskomnadzor, included the service in its register of banned resources but never managed to block its operation on Russia's territory. It is not clear how negotiations between Yandex and the FSB ended; Yandex Managing Director Tigran Khudaverdyan stated that the company "has a solution to the problem" but did not disclose the details.[196] In the first half of 2020, Russian government agencies sent Yandex more than 15,000 requests for users' information, of which Yandex reportedly fulfilled 84 percent.[197]

Russia has also announced plans to isolate Internet traffic within Russia from the world's Internet, creating something called the RUNET. This would serve several functions: to allow Russian telecommunications equipment companies exclusive rights to the Russian market, so they would not be forced to compete with international products; to facilitate the monitoring and intercept of traffic within Russia; and to prevent unwanted external content from reaching a Russian audience. This continues to be an aspirational goal, although the Russian government claimed to have conducted a successful test of the RUNET in 2019.[198]

CONCLUSION: STRENGTHENING INTERNAL SECURITY

Internal security is the highest priority of Russian intelligence and state security services. Multiple services, including the FSB, FSO, and National Guard, use all available tools, including human and technical platforms, to neutralize threats to the ruling regime. Russia has intensified its use of technical methods to monitor the domestic communications environment, making thousands of requests for Internet users' information, to meet a mix of all three major internal security missions: counterintelligence, counterterrorism, and suppressing internal dissent. Russia is even working toward isolating the Russian Internet from the rest of the world to facilitate operational and investigative measures as well as to prevent Russians' minds from being tainted by foreign thinking. Although some of the threats that Russia sees in its society have Western analogues, such as foreign intelligence services and terrorist groups, Russia's pursuit of internal security encompasses threats from the domestic Russian population, which most countries would consider legitimate opposition. At the same time, Russian services are constantly seeking, and claiming to have found, foreign connections to internal threats, whether they exist or not.

CHAPTER 4

POLITICAL INTELLIGENCE COLLECTION

Political intelligence is the traditional type of foreign intelligence that has existed across governments and time. The purpose of political intelligence is to support political and foreign policy decisionmaking. In Russia, that purpose has remained consistent from the Soviet era to today.

Alexander Orlov called "diplomatic intelligence" the most important of his eight types of Soviet intelligence, with its purpose being "… to keep the Soviet government informed of the secret deals between governments of capitalistic countries and of the true intentions and contemplated moves of each of those governments toward the Soviet Union."[199] KGB defector Oleg Gordievsky similarly defined this category of intelligence 30 years later, asserting that "information from the intelligence service must assist our authorities to reach optimum foreign policy decisions."[200] When discussing a political intelligence incident in the UK in 2011, an official of MI5, the UK's counterintelligence and security agency, stated that Russia defines political intelligence as information that would "enable Russia to formulate policies which win maximum advantage in the light of insights gained from intelligence."[201] The U.S. Intelligence Community calls this "decision advantage."[202]

When Gordievsky defected in 1985, he brought materials that identified Soviet intelligence priorities during the previous several years, including a Soviet intelligence document that advised: "Begin from the assumption that the United States is trying to secure a dominant position in the world regardless of the interests of other states and nations."[203] Gordievsky disclosed that the head of the KGB First Chief Directorate, Vladimir Kryuchkov, had directed Soviet intelligence in 1983 to uncover U.S. and Allied plans to dominate the world and conduct subversive activities in the Soviet zone of control. An American nuclear attack was especially high on the minds of Soviet national security policymakers, who viewed every U.S. move through the lens of a potential nuclear war. As one of the two superpowers, the Soviet Union also needed to monitor hot spots in other parts of the world, like the Middle East and South Asia, the Non-Aligned Movement, and the Vatican, although those intelligence targets were often founded on perceived nefarious U.S. intentions.[204]

The United States and its allies remain the main targets of Russian political intelligence today just as they were during the Cold War. The 2016 Foreign Policy Concept of the Russian Federation articulated a similar theme, identifying Russia's primary adversary and its allies with phrases like "unipolar power" and "western powers."

> Western powers' attempts to maintain their positions in the world, including by imposing their point of view on global processes and conducting a policy to contain alternative centres of power, lead to a greater instability in international relations and growing turbulence on the global and regional levels. The struggle for dominance in shaping the key principles of the future international system has become a key trend at the current stage of international development.[205]

A comparison of Cold War-era Soviet intelligence priorities with recent Russian intelligence operations reveals notable continuity (see Figure 8). U.S. and NATO political intentions remain high on Russia's list, but with two key differences. One is the redefinition of Russia's sphere of influence

Figure 8. **Comparison of Soviet and Russian Intelligence Priorities**

KGB Priorities for 1984	Current Russian Intelligence Priorities
Inform Soviet and Eastern Bloc foreign policy steps to limit and reduce nuclear missiles and other weapons of mass destruction	Monitor Western weapons development and defense policy, especially vis-a-vis Russia
Monitor U.S. and allied preparations to launch a surprise nuclear attack on the Soviet Union	Monitor U.S. military plans toward Russia
Monitor the principal aspects of U.S., Western European, and Japanese strategies toward the Soviet Union	Monitor U.S. and allied diplomatic foreign policy toward Russia
Monitor the plans and subversive actions by the main enemy towards weakening the unity of the countries of the socialist community	Monitor U.S. and allied foreign policy toward the Near Abroad
Monitor the development of events in areas where crisis situations exist, especially in the Middle East and Afghanistan	Develop liaison relations with countries in the Middle East and South Asia
Monitor the internal political situation in the United States	Monitor the internal political situation in the United States
Monitor China's foreign policy and its approach to Sino-Soviet relations	Keep China as a close ally
Monitor the activities of the Non-Aligned Movement, the Socialist International, the Vatican, and Islamic states	Monitor Africa, Latin America, and the Middle East

Sources: Figure created by author from multiple sources, including Christopher Andrew and Oleg Gordievsky, Comrade Kryuchkov's Instructions: Top Secret Files on KGB Foreign Operations, 1975-1985 *(Stanford, CA: Stanford University Press, 1993); Ministry of Foreign Affairs of the Russian Federation,* Foreign Policy Concept of the Russian Federation*, December 1, 2016; and multiple Russian intelligence operations discussed below.*

from the Warsaw Pact during the Cold War to the Near Abroad in the post-Cold War era. As Russia lost the Warsaw Pact alliance at the end of the Cold War, its priorities shifted from employing Warsaw Pact countries to its political advantage, to viewing them as NATO and European Union adversaries. Consequently, Russia was forced to retrench closer to the borders of the former Soviet Union, while even those borders are insecure. The other difference is the place that China occupies in Russian intelligence targeting. Beginning in the 1960s, the Soviet Union perceived China as a competitor, and Soviet intelligence treated it as a threat. Today, although Russia has probably not forgotten that history altogether, its public objectives include keeping China close to avoid surprises and to tap into China's political and economic might in the world.

Russian political intelligence collection targets the policymaking establishments of foreign countries. Prominent among Russian political intelligence targets are ministries of foreign affairs, corresponding with Orlov's label "diplomatic intelligence" to describe political intelligence. Policymaking targets also include ministries of defense and NATO. Russia seeks intelligence about foreign countries' strategic plans and future capabilities, including plans for a surprise attack and principal aspects of strategy—just as in the 1984 KGB priorities—to inform Russia's political leadership about possible countering moves in the political realm. Intelligence collection to support tactical military decisionmaking and covert operations is discussed in Chapter 6.

Russia views its political reputation in the world as a national security priority, in relation to perceptions of its relative power and ability to coerce other countries and to the credibility of the ruling elite within the Russian domestic political environment. In Putin's perception, a Russia that appears to be weak is a vulnerable Russia. As he wrote in 2012: "We should not tempt anyone by allowing ourselves to be weak… Falling behind means becoming vulnerable."[206] Putin's 2012 statement echoed Stalin, who reportedly said nearly 90 years earlier, "The Soviet Union must never be toothless and groveling before the West again."[207] Thus, Russian intelligence organizations are tasked to track hot, current topics related to Russian interests, including investigations involving Russian actions or NATO membership discussions. When Russia is publicly criticized for activities, such as using a dangerous chemical weapon in a public place on another country's sovereign territory, sheltering Syria's use of chemical weapons, running a concerted doping program for its athletes competing in international sporting events, or supplying the weapon that shot down a civilian airliner, it uses its political intelligence collection capability to monitor those discussions and inform Russia's response.

Russian disinformation operations and so-called "hybrid warfare" have received much publicity since Russia's illegal annexation of Crimea in 2014. Although these covert operations could not proceed without political intelligence to identify specific targets and exploitable themes—Russia uses every tool available to denigrate its adversaries and build its own military and political power—political collection operations are separate from covert and disinformation operations. Covert operations and political collection are conducted by different organizations within the Russian intelligence system, and the two types of operations serve mostly different purposes. While some information derived from traditional political intelligence collection operations can be repurposed for disinformation or influence operations, such covert missions are not the sole reason for that collection.

The role of political intelligence in Russian operations is further illustrated in a database that the Council on Foreign Relations (CFR) has compiled of over 350 government-sponsored computer intrusion incidents and computer-network attack incidents dating back to 2005.[208] Eighty-four of those incidents are attributed to a Russian government-affiliated threat actor. For comparison purposes, the CFR attributes 129 incidents to China, 36 to Iran, and 28 to North Korea, with 41 others distributed among 24 different countries.

Of the 84 operations attributed to Russia, the majority appear to target political collection targets: defense, diplomatic, election, and other government computer systems or think tanks that advise governments. Eight of the Russia-related incidents target sports regulation organizations or organizations that monitor doping among athletes, a target of particular political importance to the Russian government's reputation abroad. Six others target journalist and media organizations, particularly those that publish information about Russian malign political actions. Although political collection is most prominent among these operations, 10 of the incidents also target infrastructure control systems, including electricity generation, water distribution, and transportation infrastructures, which are either related to the ongoing military conflict in Ukraine or have a contingency motive in case of future military conflict with another world power (see Chapter 6).

TARGETING MINISTRIES OF FOREIGN AFFAIRS

Ministries of foreign affairs have been the continuous target of Russian intelligence operations since the Soviet era. SVR Line PR continues to be the largest section in *rezidenturas* around the world, meaning that political intelligence, particularly directed at diplomatic entities, is still a high priority. These activities are intended to get inside information about foreign countries' political moves, especially as they relate to Russia, but also to Russia's allies and diplomatic partners, such as China, Venezuela, Syria, and Iran. Russian intelligence services use a spectrum of methods to penetrate ministries of foreign affairs, from close access SIGINT and human recruitment to computer-network collection, conducted by a combination of SVR and GRU officers.

HUMINT

As was typical during the Soviet era, human targeting is the predominant method Russia uses in political collection operations. Russia relies heavily on human sources for political collection around the world. Sergey Tretyakov, the SVR deputy *rezident* (chief) who operated under diplomatic cover at the Russian Mission to the United Nations during the 1990s, described Russian recruitments of diplomats from various countries, including Germany, Greece, Poland, Sweden, Tajikistan, Turkey, Uzbekistan, and an unspecified African country.[209] These foreign diplomats, some of whom may not have even realized they were Russian intelligence sources, provided a variety of information about U.S. political actions, other countries' relations with the United States, NATO political and military discussions, Central European countries' aspirations for NATO and European Union membership, and other similar topics. Tretyakov's biographer, Pete Earley, described the United Nations as a "big candy store" for SVR officers.[210]

Russian illegal intelligence officer Lidiya Guriyeva (aka Cynthia Murphy) sought to cultivate access to an associate of the U.S. Secretary of State in 2009.[211] Guryeva and her husband Vladimir Guriyev (Richard Murphy) had been dispatched to the United States in the mid-1990s, and they operated for nearly 15 years until their arrest in 2010. When Guryeva reported her contact, Moscow responded that the individual was a "very interesting target" and that she should "try to build up little by little relations with him moving beyond just [work]," because he might be able to supply "remarks re U.S. foreign policy" as well as "'rumors' about White House internal 'kitchen.'"[212] The word "kitchen" in Russian can refer to office politics or internal gossip. After this connection became public in 2010, then-Secretary of State Hillary Clinton issued a public statement that there was "no reason" to think the secretary was a target of the illegals.[213] However, secretaries of state and ministers of foreign affairs are routine targets of Russian political intelligence collection. Being a target does not mean being a spy—Russian intelligence typically targets potential recruits surrounding such a high-level target, with the secretary or minister only seldom becoming the actual recruited agent. The targeted individual may not even realize the cultivation is taking place.

Russia actively cultivates sympathetic politicians who not only have access to sensitive political information but also are willing to present a Russia-slanted picture of events, particularly focused on the EU. In 2018, a Hungarian politician from the right-wing Jobbik Party, Bela Kovacs, was arrested and charged with espionage. He reportedly provided "information on a range of European Union matters connected to Russia, including details about energy negotiations, relations with Belarus, the future of the European bank sector and a possible EU visa waiver for Russia."[214] A Bulgarian politician, Nikolai Malinov, was arrested in 2019 for providing information about Bulgarian political decisionmaking related to Russia and Europe. Malinov, the leader of a pro-Russian group in Bulgaria called the Russophiles National Movement, also allegedly took part in an attempt to exert influence on the Bulgarian government's foreign policy toward Russia and the West. One of the documents Malinov provided "outlines the steps needed to be taken to completely overhaul the geopolitical orientation of Bulgaria away from the West towards Russia." Russian representatives called the arrest an American-sponsored spy fiction.[215]

Close Access SIGINT and Computer Intrusions

Catching Russian intelligence officers in the act of close access SIGINT operations is a relatively rare occasion. Several incidents have been publicized, however, that focused on political collection. In 1999, the FBI arrested Stanislav Gusev, a Russian embassy officer who was caught servicing a transmitter implanted in a chair rail in a conference room of the U.S. State Department in Washington, DC.[216] The FBI seized the equipment that Gusev was using to control the implanted microphone and expelled him from the country. According to U.S. press reporting, the bug allowed the Russian intelligence service to "capture a wide variety of information, much of it classified,"[217] but as of 2021, no information is publicly available to explain how or when the microphone was emplaced.

Although intended to be clandestine, at least three close access technical operations have been identified publicly since 2018. One targeted a diplomatic gathering, the World Economic Forum (WEF) in Davos, Switzerland, in 2019. Swiss police arrested two Russians carrying diplomatic passports, one of whom was posing as a plumber, near the WEF venue. Swiss press sources described the two men's activity as "preparatory work for spying on the World Economic Forum," adding that the Russians "had their sights on the WEF" and might have planned to conduct electronic surveillance of the summit.[218] Two other close access collection incidents occurred in 2018 in Norway and the Netherlands, when Russian intelligence officers were caught with signal intercept equipment in or near the Parliament building in Norway and the Organization for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. These incidents will be discussed in more detail in Chapter 9.

Computer-based Collection

Computer network operations are particularly prevalent against ministries of foreign affairs around the world, either because the ministries are soft targets or because they have competent computer security monitoring that catches penetrations (see Figure 9). As in many computer collection ventures, the victim's choice to make it public carries some cost because the penetration can highlight systemic vulnerabilities, although those are often mitigated with the assistance of computer security personnel.

Figure 9. Reported Russian Computer Incidents Targeting Ministries of Foreign Affairs

2009–13: Finland—Computer penetration at foreign ministry

2013–14: United States—Computer penetration at State Department and White House

2015–16: Denmark—Computer penetration at foreign ministry

2016: Multiple—Spearfishing campaign targeting foreign ministries

2016: Italy—Compromised email communications between Rome and missions abroad

2016: Czechia—Compromised electronic communications; two parallel attacks

2016–17: Multiple Eastern European countries—Computer penetrations in consulates and embassies

2017: North America and Europe—Spearphishing attack on two foreign affairs government institutions

2017: Czechia—Computer penetration attempt at foreign ministry

2017: Romania—Spearphishing campaign targeting foreign ministry

2018: Germany—Computer penetration at federal foreign office

2018: United Kingdom—Foreign and Commonwealth offices targeted by computer intrusion attempt

2018: South Korea—Foreign ministry and financial institutions target of computer intrusion attempt

2019: Eastern Europe and Central Asia—Spearphishing campaign targeting embassies and foreign ministries

2020: Armenia—Computer penetration of the consular section of the Armenian embassy in Moscow

2020: United States—Massive computer intrusion using SolarWinds computer management software penetrated multiple U.S. Government entities, including the U.S. Department of State, seeking intelligence on U.S. policies toward Russia

Sources: Figure created by author from multiple sources, including Anthony Cuthbertson, “Chinese and Russian Hackers ‘Targeting South Korea Ahead of US-North Korea Summit,’” The Independent*, June 5, 2018,* https://www.independent.co.uk/life-style/gadgets-and-tech/news/trump-us-north-korea-summit-kim-jong-un-hackers-china-russia-a8384586.html*; Sean Lyngaas, “Russian Intelligence-Backed Hackers Go After the Armenian Embassy Website with New Code,” Cyberscoop.com, March 12, 2020,* https://www.cyberscoop.com/turla-fsb-eset-armenia/*; “Joint Statement by The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA),” January 5, 2021,* https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure*.*

Regardless of the method—SIGINT, human, or computer network collection—Russian intelligence activities targeting ministries of foreign affairs worldwide reflect Russia’s high priority for monitoring foreign policy establishments.

TARGETING DEFENSE AND SECURITY POLICY INFORMATION

Understanding other countries' defense policies is especially important for Russia, given its underlying suspicion that the West intends to harm Russia. Countries that are already NATO members, as well as those that aspire to NATO membership, are at the top of the target list for penetrating defense establishments. Russian targeting of defense establishments has several goals, namely to identify:

- Conventional military plans, especially as they involve potential attacks on Russia.
- Strategic nuclear plans.
- Future weapons systems that Russia will need to counter.
- People who can serve as influence or penetration agents.

These topics have both political and military relevance, and intelligence on them can support Russia's political actions vis-a-vis the United States and NATO.

HUMINT

Between 2008 and 2020, at least 14 foreign nationals serving as Russian intelligence agents were arrested for providing NATO policy and defense information to the SVR or GRU (see Figure 10). Russian intelligence agencies recruited these agents across a 20-year span of time, beginning during the Soviet era and continuing to at least 2009. One of the agents, Martin Möller, was recruited in the 1980s while serving as a member of the United Nations Iran-Iraq Military Observer Group (UNIIMOG) in Tehran, Iran;[219] he was handled by the GRU. Two others were recruited in the 1990s. The SVR recruited Herman Simm in about 1995, and he gave the SVR access to intelligence about Estonian, NATO, and EU information security procedures.[220] Recruited in 1996, Peter Debbins realized he was working for the GRU by 1999. He served as an army officer from 1998 to

2005 and, although he had little access to information of interest to Russia from 2005 to 2010, he gained access to classified information as a contractor from 2011 until his arrest in 2020.[221]

Figure 10. **Arrests of Individuals Working in Ministries of Defense**

2008: Estonia—Herman Simm, chief of Estonian Defence Ministry Security Department

2012: Canada—Jeffrey Delisle, Canadian Navy officer working in NATO intelligence fusion center

2013: Netherlands—Raymond Poeteray, Dutch diplomat with access to NATO and EU policy information

2018: Austria—Martin Möller, Austrian military officer with access to Austrian interactions with NATO

2019: Poland—Arrest of individual working for a contract company that supported the Defense Ministry's Agency for Military Property

2019: Lithuania—Arrest of Romanas Šešelis for collecting information for Russia on NATO military ships, an LNG terminal company, and other infrastructure

2020: United States—Peter Debbins, former U.S. Army officer who worked in various IC-related contracting companies

2021: Bulgaria—Six Bulgarians arrested for providing classified defense information to Russian intelligence officers in Bulgaria

2021: Italy—Italian Navy captain arrested for providing defense and national security policy information to Russian diplomatically covered officers

Sources: Figure created by author from multiple sources, including U.S. District Court, Eastern District of Virginia, "USA vs. Peter Rafael Dzibinski Debbins, aka 'Ikar Lesnikov'," August 20, 2020, https://www.justice.gov/opa/press-release/file/1307186/download*; "Bulgaria: Six arrested over 'Russian spy network,'" DW.com, March 19, 2021,* https://www.dw.com/en/bulgaria-six-arrested-over-russian-spy-network/a-56934658*; Crispian Balmer and Angelo Amante, "Italy arrests navy captain for spying, expels Russian diplomats,"* Reuters*, March 31, 2021,* https://www.reuters.com/article/uk-italy-russia-spies-idAFKBN2BN0W4*.*

Russia recruited other intelligence agents during the Putin era. Jeffrey Delisle walked into the Russian embassy in Ottawa in 2007 and was recruited by the GRU. Delisle had access to classified computers that contained data from the Privy Council Office—responsible for the day-to-day planning of the Canadian government—the Canadian Security Intelligence Service, and the Royal Canadian Mounted Police, as well as Five Eyes Coalition and NATO intelligence. He admitted that much of what he provided was SIGINT-derived intelligence.[222] Raymond Poeteray, who was recruited in 2009, provided information about NATO activity in Libya, EU fact-finding missions in Georgia, and Dutch peacekeeping missions in Kosovo and Afghanistan. SVR illegals Andreas and Heidrun Anschlag, who lived in Germany, handled Poeteray.[223] A Polish official arrested in 2019, identified publicly only as Piotr Ś., had access to Polish and NATO information, particularly about construction projects at the Multinational Division North East Headquarters, which coordinates the activities of NATO Enhanced Forward Presence battle groups deployed in the Baltic states and Poland.[224] The timing of his initial recruitment is unclear, but he probably was handled by the GRU.

During the same 20-year timeframe, a number of Russian intelligence officers were arrested, expelled, compromised, or disappeared after targeting defense policy information in multiple countries. In some cases, the identities of the agents they were running are not publicly available, but their targets are consistent (see Figure 11).

Figure 11. Russian Intelligence Officers Targeting Defense Information

2009: Poland—Russian nonofficial cover (NOC) officer who had contact with defense officials was arrested.

2009: United States—Illegals Michael Zotolli and Natalya Perevezeva (aka Patricia Mills) moved into an apartment near the Pentagon, where many of their neighbors were Department of Defense officials.

2010: Spain—Illegal Sergey Cherepanov (Henry Frith) disappeared; his targets reportedly included intelligence on Croatian NATO membership.

2011: Germany—Illegals Andreas and Heidrun Anschlags were arrested; they were later revealed to be running Raymond Poeteray.

2011?: France—Russian embassy officer "Vladimir F." quietly expelled for targeting parliament members for defense and security information.

2012: Canada—Russian embassy officers expelled for Delisle case; the Russian embassy denied its officials had been expelled and claimed they left Canada on a normal rotation.

2014: Canada—LtCol Yuriy Bezler expelled for reasons related to Russian actions in Ukraine.

2016: Hungary—One GRU officer was expelled for activities not publicly described but reportedly related to NATO.

2018: Slovakia—A Russian diplomat was expelled "for engaging in intelligence activities against Slovakia and NATO."

2020: Bulgaria—Russian military attaché was expelled for collecting sensitive military information, including about U.S. troops deployed to Bulgaria.

2021: Bulgaria—Two Russian diplomats were expelled for running an espionage network within defense circles.

2021: Italy—Two Russian diplomats were expelled for espionage involving an Italian Navy captain with access to defense and national security policy information.

Sources: Figure created by author from multiple sources, including Laura Stone, "Canadian Diplomat Expelled From Russia," Global News*, April 22, 2014,* https://globalnews.ca/news/1284073/canadian-diplomat-expelled-from-russia/*; Panyi Szabolcs, "Russian Diplomats Caught Spying in Hungary Get Expelled Quietly as Usual," Direkt36 (Hungary), December 20, 2018,* https://www.direkt36.hu/en/orosz-diplomatakat-ertek-kemkedesen-magyarorszagon-es-szep-csendben-ki-is-szoritottak-oket/*; "Slovak PM Says Russian Diplomat Expelled For Spying,"* Radio Free Europe/Radio Liberty*, December 5, 2018,* https://www.rferl.org/a/slovak-pm-says-russian-diplomat-expelled-for-spying/29639128.html*.*

Sometimes the targeted country does not report its expulsions publicly to avoid embarrassing Russia; they are occasionally revealed years later when journalists find out about them. Nevertheless, the publicized expulsions show a continuing human-based effort to collect defense policy information.

Computer-based Collection

In addition to these human penetrations, numerous Russian computer intrusion incidents have been reported targeting ministries of defense, including several incidents of penetrations or attempted penetrations into U.S. computer systems (see Figure 12).

In some cases, the target's computer security systems detected and interdicted Russia's computer penetration attempts before they accessed any sensitive data; in other cases, Russia gained access to the targeted networks. Either way, these computer-based operations, in concert with continual HUMINT operations, represent a consistent Russian campaign to collect defense-related policy information. Both human and technical collection efforts are valuable. While computer-based operations can yield information that is sensitive but unclassified, human penetrations offer access to classified files that computer penetrations often cannot reach.

Figure 12. Russian Computer-Based Operations Targeting Ministries of Defense

2008: United States—DoD computers penetrated ("Buckshot Yankee")

2014: Ukraine—Ministry of defense computers penetrated, allowing the insertion of false information into the system

2015 (early in the year): United States—Computer penetration of DoD networks

2015 (July): United States—Computer penetration of DoD networks

2015–16: Denmark—Computer penetration into Danish defense ministry

2016: Czechia—Computer penetration attempts target Czech Republic defense ministry

2016–17: Multiple—Computer penetration attempts target defense-related organizations

2017: Montenegro—Computer penetration of government networks related to NATO accession

2017: Germany—Computer penetration into German defense ministry

2018: Czechia—Compromise of personal emails of armed forces personnel

2018: European government organization—Spearphishing campaign using defense-related bait

2018: United Kingdom—Computer penetration attempt at Defence and Science Technology Laboratory

Sources: Figure created by author from multiple sources, including "From Espionage to Cyber Propaganda: Pawn Storm's Activities over the Past Two Years," TrendMicro*, April 25, 2017,* https://www.trendmicro.com/vinfo/in/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm*; "Introducing WhiteBear," Kaspersky SecureList, August 30, 2017,* https://securelist.com/introducing-whitebear/81638/*; National Cyber Security Centre, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," October 3, 2018,* https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed*.*

TARGETING ELECTIONS

Foreign elections are a consistent target of Russian intelligence collection because elections offer a window into a country's policies and leadership. Although much Western media coverage has surrounded Russian covert manipulation of elections, the incidents in Figure 13 reflect intelligence collection activities, not meddling. Even in widely publicized cases of covert election meddling, such as in the United States, Great Britain, and Spain, Russia's intelligence collection preceded covert action, although the intelligence collection was not always publicly visible. Elections are an important Russian political intelligence target because they identify:

- **The views of the incoming administration regarding Russia.** Years before the now-famous computer intrusions, illegals in the United States were tasked with collecting information about the newly elected Obama administration, focusing on important foreign policy issues.[225]
- **Individuals on the new team who might be amenable to Russian views or strategies or who could serve as influence agents.** In the United States, the 2019 Mueller Report on the Investigation into Russian Interference in the 2016 Presidential Election discussed this potential in excruciating detail.[226] Although some of the individuals that Russian intelligence targeted may not have progressed to the point of being recruited agents, these incidents offer insights into Russian political collection priorities.
- **Potentially damaging personal information that could be used should Russia choose to discredit a foreign leader.** The Steele Dossier, alleging cooperation between the Trump presidential campaign and Russia in 2016, is alternatively characterized in the press as political opposition research or a component of Russian disinformation.
- **Themes and divisions that could be exploited in disinformation campaigns.** Inside Russia, elections are more theater than real voter choice. Thus, as Russia views elections in other countries, it mirror-images them as representing the insincere government engineering that occurs inside Russia.

Most of the publicly available examples of targeted foreign elections since 2014 involve computer-based operations, although Russia also continues to use human platforms. While Russia may repurpose the information collected in these operations for covert election meddling, such intelligence may also support Russian political and foreign policy decisionmaking. While multiple cases of collection of election-related information have targeted the United States, the United States is not Russia's only target.

Figure 13. **Russian Intelligence Operations Targeting Elections**

2009: United States—The SVR tasked illegals (Guryevs/Murphys) to collect information about newly-elected U.S. President Barack Obama's views on START, Afghanistan, and Iran

2014: Ukraine—Computer intrusions into Election Commission

2016: United States—Computer intrusions into Democratic National Committee

2016: United States—Senator Marco Rubio's office targeted by computer intrusion attempt

2016: United States—Computer intrusions into Arizona, Illinois, and Florida election systems; 18 others targeted

2016: Montenegro—Computer intrusions on the day of parliamentary elections

2017: France—President Emmanuel Macron's office targeted by spearphishing campaign

2017–20: Bulgaria—Russian embassy officers expelled for collecting information about the electoral process

2018: United States—Senator Claire McCaskill's office targeted by computer intrusion attempt

2018: United States—Democratic National Committee targeted by computer intrusion attempt

2019: Libya—Wagner Group employees arrested for attempting to influence elections in Africa

2019: Indonesia—Computer intrusions into voter database

Sources: Figure created by author from multiple sources, including Viriya Singgih, Arys Aditya, and Karlis Salna, "Indonesia Says Election Under Attack From Chinese, Russian Hackers," Bloomberg, *March 13, 2019,* https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers*; David Ingram, "Democratic Senator Alleges Russian Hackers Unsuccessfully Tried To Access her Computer," NBC News, July 26, 2018,* https://www.nbcnews.com/news/us-news/democratic-senator-alleges-russian-hackers-unsuccessfully-tried-access-her-computer-n895131*; Missy Ryan and Sudarsan Raghavan, "Russians Arrested as Spies in Libya Worked for Russian firm Wagner, Official Says,"* Washington Post*, November 18, 2019,* https://www.washingtonpost.com/world/national-security/russians-arrested-as-spies-in-libya-worked-for-russian-firm-wagner-official-says/2019/11/18/c0cee91a-0a21-11ea-a49f-9066f51640f6_story.html.

Examples of Russian penetrations into election-related computer systems in the United States have been widely publicized. The Democratic National Committee was the target of a computer intrusion before the U.S. election in 2016 that led to the theft of emails, some of which were leaked to embarrass the Hillary Clinton campaign. Other intrusion attempts reportedly targeted the Democratic National Committee, along with individual members of the U.S. Congress, in 2018. Because U.S.-Russian relations have been particularly sour since 2014, the United States probably publicizes such activities more than other countries. Computer intrusions into election databases have also been reported widely in the United States, but similar actions have been reported in Montenegro and Indonesia. Other cases of Russian intrusions into election databases have probably occurred and either gone undetected or unreported.

TARGETING LEGISLATIVE BODIES

Russian political collection operations have also targeted legislative bodies, including members of parliaments and their staffers. Like the efforts that target other decisionmaking bodies, operations that target parliaments are both to collect information about a country's priorities and future policies, especially as they relate to Russia, and to identify individuals—such as elected officials or their staff members—who could become influence or penetration agents. These activities can at times also yield classified information. Like the operations discussed above that have targeted ministries of foreign affairs and defense, Russia's targeting of other countries' legislative bodies covers the spectrum of collection platforms, from embassy-based officers cultivating human sources to computer-based operations and close access technical operations.

Penetrating parliaments has long been an objective of Soviet and Eastern Bloc intelligence services. Fred Rose, a member of the Canadian Parliament, was recruited as a Soviet source in the 1930s, and then, after serving a brief time in jail for subversive activities, he contacted the GRU *rezidentura* in September 1942 and again offered his assistance.[227] Rose was already serving as a GRU agent when he was elected to the Canadian Parliament in August 1943 and reelected in June 1945.[228] In addition to being the hub of a source network, Rose provided information on parliamentary and political matters, including the details of a closed session of Parliament that occurred near the end of 1944.[229]

Soviet intelligence defector Oleg Kalugin claimed that the KGB considered planting an electronic eavesdropping device in the U.S. House of Representatives' Armed Services Committee in 1967, but the FBI interdicted the device before it transmitted any information.[230] The KGB also reportedly increased the number of agents it had recruited in the Sri Lankan Parliament in the 1980s.[231] Other Eastern Bloc services, such as the Czechoslovakian, also enjoyed success in recruiting members of parliaments during the Cold War. The Czechoslovakian service ran a West German member of the Bundestag, Alfred Frenzel, for seven years until his arrest in October 1960.[232] Czechoslovakian state security archives also indicate that four members of the British Parliament worked as intelligence sources in the 1960s and 1970s.[233]

HUMINT

Several Russian operations targeting members of parliament have been reported in the United Kingdom during the Putin era, probably reflecting the British government's willingness to publicize the incidents rather than a particular Russian attention to the United Kingdom. In 2008, a member of the British Parliament, Andrew MacKinlay, was censured for meeting on multiple occasions with Alexander Polyakov, a suspected SVR officer covered as a counselor at the Russian embassy in London. Over the year of his meetings with Polyakov, MacKinlay posed a series of Russia-related parliamentary questions in the Commons that had a clearly pro-Russia slant: for example, why had Britain granted political asylum to Boris Berezovsky, an exiled enemy of then-Prime Minister Putin. Berezovsky had been close to Putin critic Aleksandr Litvinenko, who was poisoned in London in 2006. MacKinley's questions also addressed the number of accredited Russian diplomats, extradition provisions between the United Kingdom and Russia, and the circumstances surrounding the 2007 deportation of a Russian suspected of plotting to murder Berezovsky.[234]

Another diplomatically covered SVR officer in London, Mikhail Repin, circulated from 2009 to 2011 in security and defense circles looking for potential recruits who could provide information about British defense issues. Repin joined influential international think tanks focused on political and military affairs, where he socialized with several British members of Parliament who had access to defense-related policy information.[235]

Also in the UK, a young Russian national named Katia Zatuliveter was arrested in 2010 on espionage charges, based in part on her ties to a British legislator. Zatuliveter was both an aide to and the mistress of a member of the British Parliament who served on the British delegation to the Western European Union and the Council of Europe, as well as the Defence Select Committee in the House of Commons. She was also being cultivated by a Russian embassy officer in London identified only as Boris, who was expelled from the United Kingdom in 2011. Boris reportedly told her that she had a "dream job." Zatuliveter was acquitted of espionage in December 2011; she was probably a target of opportunity who had access to political information and whom an enterprising SVR officer noticed and tried to recruit. Whether she was guilty of espionage or not, the incident shows that a Russian intelligence officer was targeting an MP's aide.[236]

Mariya Butina may have been a similar target of opportunity in the United States, although her connections to Russian intelligence are circumstantial. Butina overtly circulated in U.S. gun rights circles from 2011 to 2018, while in close association with multiple Russian individuals with suspected ties to Russian intelligence services. Throughout these years, for example, she worked with Aleksandr Torshin, a member of the Russian State Duma from the United Russia Party and later the Deputy Governor of the Russian Central Bank; the U.S. Government sanctioned Torshin for playing a role in Russian meddling in the U.S. elections in 2016.[237] After traveling to the United States occasionally from Russia between 2011 and 2016, Butina arrived in the United States in August 2016 on a student visa to study at American University in Washington, DC, sponsored by Konstantin Nikolayev, a Russian billionaire businessman who served as Russian minister of transport from 2004 to 2012. Nikolayev allegedly has ties with Russian security services, although he denies the allegations.[238] While studying in Washington, DC, in January 2018, Butina met with Oleg Zhiganov, the director of the Russian Cultural Center.[239] Zhiganov also represents the Russian organization *Rossotrudnichestvo* (Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad, and International Humanitarian Cooperation), which is a direct descendant of the Soviet-era organization, the All-Union Society for Cultural Relations with Foreign Countries (VOKS).[240] VOKS was a frequent cover for Soviet intelligence officers, given its access to a fertile recruiting pool of Russian émigrés and foreigners sympathetic to Russia.[241] With these Russian connections supporting her, Butina cultivated relationships with individuals close to the Trump campaign, including political activists with congressional connections. The FBI arrested her in July 2018 on charges of being an unregistered agent of a foreign power. She pled guilty and was sentenced to 18 months in prison, and she was deported from the United States in 2019.[242]

Zatuliveter and Butina have been compared to Anna Chapman, a Russian illegal arrested in the United States in 2010 (see Chapter 8 for more details).[243] However, both were probably quite different from Chapman. There was no indication that either Zatuliveter or Butina were directly affiliated with an intelligence service, as Chapman was. Zatuliveter may have been simply a target of opportunity, as a Russian national who had developed close relations with an MP. Butina probably began by developing relations with people who shared her passion for guns but was similarly exploited for her access by a Russian government official, Aleksandr Torshin. Zatuliveter and Butina were both human agents, while Chapman was a staff member of a Russian intelligence service.

Computer-based Collection

Russia has also used technical platforms to target foreign parliaments. In 2015 and 2016, parliaments in Germany, Norway, and Turkey reported computer intrusions originating from Russia.[244] The German incident, which was detected in May 2015, resulted in a year-long penetration of the Bundestag's internal server and the loss of data. The German government subsequently also reported that an electrical maintenance worker passed the Bundestag building floor plans to a GRU officer working under diplomatic cover at the Russian embassy in Germany in 2017.[245]

After the 2016 intrusions in Norway, the Norwegian government again accused Russia of penetrating and stealing data from the Norwegian Parliament's email system in August 2020.[246] Additionally, in 2018, Norwegian authorities arrested a Russian named Mikhail Bochkarev for what probably was a close access SIGINT operation. While attending an international function at the Norwegian Parliament building, which included staffers from 34 European parliaments, Bochkarev was arrested on suspicion of using a laptop to monitor the building's Wi-Fi network.[247] Bochkarev was tried in a Norwegian court but later released and allowed to return to Russia. Unsurprisingly, the Russian government denied the allegations.[248]

TARGETING INTELLIGENCE AND COUNTERINTELLIGENCE INFORMATION

Russia is always eager to penetrate foreign intelligence and counterintelligence services. This was one of Orlov's eight primary tasks of Soviet intelligence, and the Soviet Union experienced multiple successes in penetrating the services of Great Britain, Germany, France, the United States, and many other countries during the Cold War. The year 1985 became known in the United States as the "Year of the Spy" because of the number of espionage cases revealed in that year alone, including individuals who worked for U.S. intelligence and counterintelligence services. Some of the last Soviet-era espionage cases in the United States were penetrations of intelligence services, including the CIA, NSA, and FBI. Penetrating an intelligence or counterintelligence service gives Russia a number of advantages: allowing Russia to identify spies within its midst, providing a window into another country's national security priorities, and opening access to the classified information shared with intelligence and counterintelligence services from across the targeted foreign government and its allies.

Such incidents have continued during the Putin era (see Figure 14). Most of the publicly known cases since 2000 are related to Estonia, reflecting both Estonia's aggressive counterintelligence efforts against Russia and its willingness to discuss penetrations of its security service openly. In 2019, the Estonian prosecutor general's office collaborated on a published monograph that analyzed prosecutions using Estonia's treason law. The monograph identified 20 people prosecuted under that law from 2008 to 2018, all of whom were affiliated with Russia; several cases involved penetrations of Estonia's security service.[249]

Figure 14. **Cases Involving Russian Targeting of an Intelligence or Counterintelligence Service**

2001: United States—50 Russian diplomats were expelled in retaliation for Robert Hanssen case.

2012: Canada—Russian embassy officers were expelled for Jeffrey Delisle case; the Russian embassy denied that its officials were expelled and claimed that they left Canada on a normal rotation.

2007?–12: Estonia—Estonian Internal Security Service (KAPO) officer Aleksei Dressen was arrested for providing investigative information to Russia's FSB.

2002–13: Estonia—Vladimir Veitman was arrested for providing information about Estonian intelligence and counterintelligence software.

2013: United States—Russia obtained access to information about U.S. intelligence collection capabilities from Edward Snowden.

2014: Estonia—KAPO officer Uno Puusepp defected to Russia; he had been cooperating with Russia for over 20 years.

2019: Estonia—Dual Estonian-Russian citizen Dmitri Kozlov was arrested for providing Russia with information on the Estonian police department's activities, employees, and equipment.

2012?–19: Estonia—Retired KAPO officer Vladimir Kulikov was arrested for cooperating with Russian intelligence.

Sources: Figure created by author from multiple sources, including Ivo Juurvee and Lavly Perling, Russia's Espionage in Estonia: A Quantitative Analysis of Convictions *(Tallin: International Centre for Defence and Security, 2019); Ian Austen, "Russian Envoys Leave Canada After Officer Is Accused of Spying,"* New York Times*, January 20, 2012,* https://www.nytimes.com/2012/01/21/world/americas/russian-diplomats-leave-canada-as-spy-case-heats-up.html.

However, Estonia is not the only target. Canada's Jeffrey Delisle, also listed earlier as a source of defense/NATO collection, worked in a NATO intelligence fusion cell where he had access to intelligence in support of NATO activities. The United States has also been affected by penetrations of its intelligence apparatus through Robert Hanssen, although most of his activities occurred during the Soviet era, and Edward Snowden, who volunteered his information to Russia, causing massive damage to U.S. intelligence collection.

Other such cases have almost certainly occurred around the world. Although some targeted countries do not openly discuss penetrations of their intelligence and security services, Russia has not stopped attempting.

HOT-TOPIC TARGETING

Russian intelligence has shown the inclination to redirect its collection apparatus toward hot topics that arise on the international stage, such as foreign investigations into Russian covert activities and NATO enlargement events. While Russia publicly denies allegations that it violates international norms, it simultaneously targets the investigations into those allegations using the whole spectrum of intelligence collection measures. Most of these incidents have occurred since 2014, possibly indicating a more aggressive Russian intelligence policy to protect Russia's image in the world.

During the several years that followed the 2006 assassination of Aleksandr Litvinenko in the United Kingdom, Russian intelligence actively sought to learn about the UK investigation of the event, as well as the follow-on investigation into allegations that Russia was targeting Litvinenko's supporter, Boris Berezovsky. As noted above, a suspected SVR officer was observed in 2007 and 2008 meeting with a member of parliament in London, probably for both collection and influence purposes. Berezovsky died in the United Kingdom in 2013, apparently of suicide, although some have questioned that determination.[250]

After the 2014 shootdown over Ukraine of Malaysian Airlines Flight MH17, on which over 200 Dutch citizens were flying, Russian intelligence targeted the Dutch government agency that was conducting the investigation. In 2015, Russian operators attacked the computers of the Dutch Safety Board, which was leading the investigation in cooperation with Malaysian, Australian, Belgian, and Ukrainian authorities and was about to present a report concluding that Russian-backed Ukrainian separatists using Russian-supplied weapons were responsible for the shootdown. The Dutch government reported multiple coordinated computer network attacks intended to obtain unauthorized access to sensitive material related to the investigation.[251] At about the same time, Russian collectors also conducted a spearphishing campaign against the investigative journalist organization Bellingcat, which was reporting information about Russia's role in the MH17 shootdown.[252]

Russia is constantly attempting to penetrate NATO through all methods to collect intelligence on NATO defense policies, and its intelligence and covert activities become especially aggressive when states are considering joining NATO. In 2017, Russian computer network operators penetrated computers in Montenegro that held data related to that country's NATO accession, using spearphishing emails that directly addressed NATO membership.[253] The following year, Greece expelled two Russian diplomats and blocked the visas of two others in retaliation for meddling in the North Macedonia naming issue. North Macedonia was formally invited to join NATO, contingent upon agreement on the country's name. Russian officers reportedly paid Greek organizations to protest the resolution to the naming issue, which further delayed North Macedonia's NATO membership. Ultimately, however, Russian attempts to derail North Macedonia's NATO accession were unsuccessful, and the country became a NATO member in 2019.[254]

When Russia and its allies are accused of using chemical weapons, Russia's immediate reaction is to deny it, while Russian intelligence services simultaneously target the resulting international investigations. Russia sided with Syria in denying allegations that the Syrian government used chemical weapons on its people in the Syrian civil war in 2017 and 2018. Russian computer operators targeted the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague and media companies as the OPCW was investigating the allegations. Russian intelligence services also targeted OPCW in reaction to allegations that GRU officers used a highly toxic chemical weapon to attempt to assassinate Sergey Skripal in the United Kingdom in 2018. In addition to these remote computer intrusion operations targeting the OPCW, as well as a chemical analysis laboratory in Switzerland, four Russian intelligence officers were arrested in the Netherlands for attempting a close access technical operation against the OPCW in 2018.[255] Bellingcat computers were again targeted in 2019 after the organization reported the identities of the Russian officers involved in the attack on Skripal.[256]

After the Russian government was accused of pursuing a concerted, government-sponsored doping program for Russian athletes competing in international sporting events, Russian intelligence targeted the World Anti-Doping Agency (WADA), which was investigating Russian athletes who benefitted from the program. Russian actors penetrated a WADA database related to the investigation and later used the collected information in a "hack and leak" operation to discredit athletes from other countries who had received legitimate exemptions for certain chemical substances on health grounds. Russia used the leaks to claim a double standard in the investigation of Russian athletes.[257]

Foreign government and private investigations have identified several Russian offices and groups, particularly affiliated with the GRU, involved in many of these cases. Considerable crossover is evident from one case to the next, including Russian intelligence officers whose names come up repeatedly across these investigations. For example, the German government issued an arrest warrant in May 2020 for Dmitry Sergeyevich Badin for his involvement in hacking into the German Bundestag in 2015. The U.S. Government indicted the same GRU officer in 2018 for conducting intrusions into the Democratic National Committee in 2016 and WADA in 2018.[258]

These incidents show how, when Russia is the subject of international allegations, Russian intelligence activities follow, both for collection purposes and in support of covert activities to discredit the investigation and turn attention away from Russia. Such activities are likely to continue, as

Russia is repeatedly caught conducting assassination operations and covert political operations around the world.

CONCLUSION: POLITICAL COLLECTION AS A PRIORITY

Political collection is a high priority for Russian intelligence. Russia sees a political motive behind many of the defense, economic, and intelligence activities of other countries. In the Russian government's calculus, if Russia can understand other countries' political drivers, it can protect itself in all other areas as well.

This calculus contains a caveat, however. Russian intelligence services have a long history of telling the boss just what he wants to hear. Russian and Soviet leaders have seldom been tolerant of an intelligence service giving them information that contradicts their firmly held political views. Stalin was known for demanding investigations into sources that provided incompatible information. Gorbachev tried to break that trend by demanding more objective information free of Cold War political assumptions,[259] but the KGB responded with lip service, as then-KGB Chairman Vladimir Kryuchkov became involved in the 1991 plot to remove Gorbachev from power. The intelligence that percolates to the Russian president today does not necessarily reflect reality as much as it reflects the president's personal preferences; as a former intelligence officer, Putin probably prefers raw information that he can analyze himself. Such selective intelligence can create a dangerous cycle of assumptions that allows only the most nefarious interpretations of world events to enter the decisionmaking process. It also leads to a cycle of aggressive Russian political moves: Russian malign actions prompt international investigations, which create more disfavor for Russia in the international environment. That disfavor feeds Russia's view that the world is against it, which leads to more aggressive actions. Russian political collection can thus be both an indicator and a driver of Russia's worldview.

CHAPTER 5

ECONOMIC AND S&T INTELLIGENCE

For Russia, economic status is a national security concern. Russia's economy relies on foreign trade to survive, and its GDP is closely connected to the oil and gas markets: as the global price of oil and gas rises and lowers, so moves Russia's prosperity. With this dependence on trade in mind, one of Russia's declared foreign policy priorities is "to create a favourable external environment that would allow Russia's economy to grow steadily and become more competitive and that would promote technological modernization as well as higher standards of living and quality of life for its population."[260]

For Russia, foreign trade also is on the same level as, and closely tied to, the development of its own military capabilities. The increase or decrease of trade income affects Russia's ability to pay for defense programs and to prepare itself for what it sees as inevitable conflict in the future. Russia also gains significant economic benefit from the sale of military weapons and nuclear power technologies. In 2012, President Putin published an op-ed that expressed the connection in his mind between Russia's military and security strength and its economic wellbeing. As he wrote in the journal *Foreign Policy* (or at least his name was attached to the article), "the huge resources invested in modernizing our military-industrial complex and re-equipping the army must serve as fuel to feed the engines of modernization in our economy, creating real growth and a situation where government expenditure funds new jobs, supports market demand, and facilitates scientific research."[261]

Thus, because Russia's economic health is key to its defense, the economy is an important national security topic against which Russia applies its national security-related agencies, including intelligence and state security. Although Russia operates openly in some economic arenas—for example, selling its oil and gas and military weapons on the open market—it often uses clandestine intelligence capabilities, even in areas where it could legally operate, under the assumption that foreign governments are cheating and stealing from Russia. Where Russia cannot operate legally—for example, in purchasing the many goods that the country cannot acquire due to international sanctions—it uses clandestine or criminal methods.

Foreign intelligence organizations, including Russian, use various methods to identify and recruit sources of economic or technological information. Those methods sometimes resemble classic human intelligence operations, in which a case officer or agent recruits a human with placement and access to the targeted information or to other people with placement and access. In 1995 the first *Annual Report to Congress on Economic Collection and Industrial Espionage* identified methods collectors used, including human intelligence methods, technical methods, and corporate methods, to collect economic and science and technology information.[262] This author was the primary drafter of that document, which was mandated by the U.S. Congress and published by the National Counterintelligence Center. A 2019 U.S. Defense Counterintelligence and Security Agency report offers a comparable list of methods that foreign intelligence institutions apply directly to U.S. companies that conduct research and development of defense technologies.[263]

A comparison of the methods described in those two documents shows many similarities across a 24-year time span (see Figure 15). They include classic agent recruitment, in which Soviet services excelled during the Cold War and which recent cases show is still being used to target economic and S&T information. Human sources include targeted individuals with desired accesses, such as Russian émigrés and employees of firms that compete with Russian companies in the international market. They also include elicitation at international conferences and trade shows, especially looking for people who have access to information or technology of value and who are willing to assist Russia.

Figure 15. **Human Intelligence Methods Used in Economic and S&T Collection**

1995 Report to Congress	2019 Targeting U.S. Technologies
Agent recruitment	Exploitation of relationship
Accepting volunteers	Exploitation of experts
Tasking employees of foreign firms	Exploitation of insider access
Headhunting, hiring competitors' employees	Résumé submission
Surveillance and surreptitious entry (hotel rooms, offices)	Surveillance
Recruitment of émigrés; inviting émigrés to return home	
Tasking foreign students	
Elicitation during international conferences and trade fairs	
Debriefing visitors to foreign countries	
Hiring information brokers and consultants	

Sources: Figure created by author from multiple sources, including National Counterintelligence Center, Annual Report to Congress on Economic Collection and Industrial Espionage *(Washington, DC: NACIC, 1995) and Defense Security and Counterintelligence Agency,* Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry *(Washington, DC: DSCA, 2019).*

Technical collection methods include computer intrusions, signals intelligence, and open-source collection, including the clandestine collection of openly available information to mask the origin of the research. Technical operations, including computer network monitoring, are the norm in the economic counterintelligence field inside Russia itself (see Figure 16). However, despite the prominence that Russian computer-network threat activity has gained in the past few years, such as for internal security and political collection, economic and technological intelligence operations abroad still rely heavily on humans, including known Russian intelligence officers and criminal groups—sometimes manned by "former" intelligence officers—that operate in the interests of the Russian government.

Figure 16. **Technical Intelligence Methods Used in Economic and S&T Collection**

1995 Report to Congress	2019 Targeting U.S. Technologies
Hacking	Exploitation of cyber operations
Communications intercepts	Exploitation of security protocol
Open-source collection; clandestine collection of open-source materials	

Sources: Figure created by author from multiple sources, including National Counterintelligence Center, Annual Report to Congress on Economic Collection and Industrial Espionage *(Washington, DC: NACIC, 1995) and Defense Security and Counterintelligence Agency,* Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry *(Washington, DC: DSCA, 2019).*

The Russian government also uses corporate methods to collect economic and S&T intelligence, such as exploiting capital investments, sponsoring foreign research activities, inviting foreign companies to set up research centers and support educational institutions in Russia, establishing joint ventures, or proposing corporate mergers and acquisitions (see Figure 17). For example, in the past several years, as Russia has emphasized research into artificial intelligence and autonomous systems, the Russian government has invited foreign firms, including industry leaders from China and South Korea, to come to Russia and set up research centers. The firms have brought their technology to Russia, sponsored training for Russian researchers, and developed joint research ventures that greatly supplement Russia's indigenous capabilities. Although these efforts are overt and legal, they are undoubtedly accompanied by at least counterintelligence surveillance of the visiting foreign researchers in Russia and probably by recruitment efforts directed at them to gain a long-term source inside the foreign company. Merging overt corporate activities with clandestine operations for intelligence and counterintelligence is a typical Russian tactic.

Figure 17. **Corporate Intelligence Methods Used in Economic and S&T Collection**

1995 Report to Congress	2019 Targeting U.S. Technologies
Foreign government use of private sector organizations, front companies, and joint ventures	RFI/Solicitation
Corporate mergers and acquisitions	Exploitation of business activity
Corporate technology agreements	Attempted acquisition
Sponsorship of research activities	Economic disinformation
	Exploitation of supply chain

Sources: Figure created by author from multiple sources, including National Counterintelligence Center, Annual Report to Congress on Economic Collection and Industrial Espionage *(Washington, DC: NACIC, 1995) and Defense Security and Counterintelligence Agency,* Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry *(Washington, DC: DSCA, 2019).*

Russian economic and technological intelligence activities demonstrate a number of these methods, from human intelligence to technical and corporate intelligence. Russia applies these methods both against foreign targets and against political oppositionists inside Russia, as will be discussed below.

Russian intelligence and state security activities related to the economic aspect of Russia's national security can be divided into three areas, each of which is organizationally distinct within the Russian intelligence system:

- Science and technology intelligence.
- Economic intelligence.
- Economic counterintelligence.

S&T COLLECTION

For Russia, science and technology intelligence, or what Orlov called "industrial intelligence," is the collection of foreign information and technological products to support the development of Russian science and technology. It focuses on the priorities and direction of Russian scientific research organizations, and it strives to raise the overall technological capacity of Russian enterprises. This collection often requires the clandestine circumvention of sanctions or foreign laws that prohibit the export of technologies to Russia, particularly targeting equipment or know-how to suppors the Russian military or security industries. The overall goal is to bolster Russia's own economic and military strength.

Both the SVR and GRU collect S&T intelligence, often competing with each other for sources and targets. The SVR has the distinct *Научно-Техническая разведка* (Directorate NTR, or Science and Technology Intelligence Directorate). This unit is the direct descendant of the Soviet-era KGB's First Chief Directorate, which had an equivalent component, then called Directorate T. Because of its focus on military technology, S&T intelligence is also a priority function for the GU (formerly called GRU).

Early Soviet Era

Historically, Soviet technology collection operations appeared in any country where technology was available, the most technologically advanced countries being the most likely to be targeted. These operations were conducted partially because Russia could acquire foreign technology more cheaply than could be done legally; partially because foreign countries placed protections on their technology, especially military-related and dual-use technology, that prohibited Russians from acquiring it legally; and partially because Russia lacked the technology base on which to develop the technology domestically.

For example, Soviet illegal Samuel Ginzberg (aka Walter Krivitsky) served in Italy in the 1920s as a Russian military intelligence officer, undercover as a scholar researching the history of slavery in the Vatican library. His intelligence mission, however, included obtaining the plans for an Italian submarine.[264] Benito Mussolini had agreed to sell the plans for an outmoded submarine model to the Soviet Union, but Stalin wanted the most recent model. In 1928, Ginzberg used a communist sympathizer to contact an Italian engineer who was willing to sell the plans.[265] For his effort, Ginzberg received the Order of the Red Banner in 1931. His network later collected the plans for a French submarine as well.[266] Similarly, a British intelligence source reported in the early 1930s that another Soviet illegal, Ignatiy Poretskiy (aka Ignace Reiss), targeted the German chemical company IG Farbenindustrie, recruiting an individual named Krupp.[267]

During the 1930s, S&T collection was the primary Soviet intelligence effort directed against the United States, which the Soviet Union saw first and foremost as a repository of technology. According to a Soviet military intelligence defector, the Soviet Union's goal in the 1920s/1930s was to "catch up to and surpass America."[268] In 1934, a Soviet illegal intelligence officer, Iosif Volodarsky, arrived in the United States to work as an assistant to Gaik Ovakimyan, an OGPU officer operating undercover as an engineer at Soviet Amtorg Trading Company in New York City. Ovakimyan had arrived in the United States a year earlier, and his operations focused particularly on scientific and technological intelligence. In December 1935, Ovakimyan openly stated that he was in the United States to "investigate American methods of producing chemicals. If I believe such methods would prove beneficial to my country and satisfactory arrangements can be made, I recommend a license be obtained so we may produce under patent rights. In some cases, we ask your manufacturers to design and sell to us chemical producing machinery."[269] Volodarsky's engineering background corresponded well with supporting this mission, which was not always as above board as Ovakimyan made it sound.

Volodarsky himself described a process through which he received technology collection requirements from Ovakimyan and dispatched an American agent to factories and engineering facilities around the United States to acquire sketches or drawings. Ovakimyan provided money to Volodarsky, and he passed it to an agent to pay sources. The agent communicated the information back to Volodarsky, who evaluated it and determined whether it met the requirement and was worth the money.[270] Volodarsky's main targets were strategic industries, such as steelworks and precision machine manufacturers, as Stalin's five-year plan stressed the need to grow the Soviet steel industry.[271]

Other advanced manufacturing technologies were targeted to support Russia's strategic industries. Orlov described Soviet intelligence efforts to steal the industrial process to manufacture artificial diamonds in Germany. The Soviet Union initially approached a German company to buy the patent legally, but the company charged an astronomical figure. Orlov quotes Stalin as saying, they "want too much money. Try to steal it from them. Show what the NKVD can do."[272]

Cold War

Among the numerous Cold War examples of economic and technological collection by Soviet intelligence services, much of the technological intelligence was destined for weapon system development, while some supported other industries, like agriculture or pharmaceuticals. In the mid-1970s, the KGB reportedly boasted about having recruited sources in 17 U.S. technology enterprises, including IBM, Texas Instruments, ITT, and the National Institutes of Health. KGB defector Vasiliy Mitrokhin provided a KGB report claiming that over half of Soviet defense industry projects in 1979 were based on Western-acquired science and technology. The chief of the KGB Directorate T—responsible for collecting technological information and the predecessor to today's SVR Directorate NTR—boasted that the value to the Soviet economy of the information his directorate collected was 100 times greater than the cost of his operations.[273]

GRU officer Vladimir Rezun (better known by his pen name Viktor Suvorov) revealed the GRU's tradecraft for targeting trade shows in Europe. In an extended description of a group of GRU officers descending on a telecommunication technology trade show in Geneva, Switzerland, in 1975, he explained how the officers looked for owners of small companies that supplied technologies to bigger weapon system manufacturers. As Rezun described, the officers launched the process of recruiting the small company owners as

GRU sources by offering the less well-off companies an opportunity to sell their products for more money than they could typically expect to get.[274]

Between 1981 and early 1982, KGB officer Vladimir Vetrov passed a series of documents to the French counterintelligence service detailing KGB technology collection efforts, which came to be known as the Farewell Dossier. Vetrov was an engineer who had been assigned to evaluate information on NATO hardware and software. Vetrov's nearly 4,000 secret documents included the complete list of 250 Line X (technology collection) officers stationed under legal cover in embassies around the world; a list of Soviet organizations involved with scientific collection; and summary reports from Directorate T on the goals, achievements, and unfulfilled objectives of the program, along with more than 100 leads to Line X recruitments.[275]

SVR officer Vladimir Konoplev operated under the cover of first secretary of the Russian Embassy in Brussels, Belgium, where he was responsible for scientific technological collection, and he shared details about his work after defecting with his family in March 1992. Konoplev reportedly had contacts inside the European Economic Community Commission, the Belgian Defense Ministry, and NATO. He revealed the names of several Belgians who were providing the Soviet Union with military and economic information, including Guido Kindt, an aerospace science correspondent for the Belgian newspaper *De Standaart*, who provided the KGB with information about technological developments in the U.S. space program.[276] Kindt subsequently reported that his handler mainly requested technical information about the places Kindt visited as a journalist: NATO SHAPE, the Belgian aircraft manufacture Sabca, and the Von Karman Institute for Fluid Dynamics, which conducted high-speed wind tunnel tests.[277]

The KGB also used SIGINT to collect S&T intelligence. According to Mitrokhin, Soviet SIGINT facilities in the United States intercepted the communications of Brookhaven National Laboratory on Long Island in New York and several major companies.[278] The SIGINT facility at the Soviet diplomatic resort on Long Island was in a position to intercept communications from the Grumman Corporation, which was involved in defense research and development. The Soviet, and later Russian, consulate in San Francisco was located on a hilltop that gave it line-of-sight access to high-tech facilities in Silicon Valley. According to a former U.S. Government official, "It was almost like everyone they had there was a technical guy, as opposed to a human-intelligence guy."[279] With the continuing use of Russian diplomatic establishments as SIGINT facilities (see Chapter 9), their use for S&T collection is a strong possibility.

In 1982, the U.S. National Intelligence Council summarized Soviet technology collection efforts as follows:

> The USSR is engaged in a well-organized, centrally directed, and growing worldwide program to acquire U.S. and other Western military technology, embargoed equipment, and manufacturing technology to satisfy its military and defense-industrial needs. The Soviet intelligence services and their Eastern European surrogates play a major role in this worldwide program through a broad range of clandestine, technical, and overt collection operations. Although these intelligence operations constitute a small part of the overall Soviet technology acquisition effort, we believe these operations are responsible for acquiring the overwhelming majority of the militarily significant Western technology that finds its way into the Soviet Union.[280]

In short, the Soviet Union had many legitimate, overt S&T relationships through which it acquired technology. But in the military technology area, it heavily used its intelligence services.

Post-Cold War

Such activities continue today on at least the same level as during the Cold War, ranging from highly sophisticated and well-funded clandestine operations to simple attempts to carry prohibited items across an international border in a suitcase. Multiple individuals have been arrested in the United States and other countries for illegally acquiring technology, with Russian military and state security agencies sometimes identified as the direct recipients. Technology collection operations in the past decade have exhibited several of the methods that the U.S. National Counterintelligence Center identified in 1995, such as investing in start-up technology companies, establishing front companies, and recruiting former employees of competitor companies as insider sources, including by embassy-based intelligence officers. Sometimes these efforts involve recruiting insiders to steal trade secrets, recruiting high-tech specialists, or establishing a business presence abroad that can act as a legitimate company while redirecting information or high-tech components to Russia.

In 2011, the Russian government-owned venture capital firm Rusnano opened operations in Menlo Park, California, and began to insert people into venture capital groups around Silicon Valley that financed nanotechnology projects.[281] Rusnano also used business investments to fund research at leading-edge technology companies, including $50 million in Boston-area nanomedicine firms. Just a few months after the United States imposed sanctions on Russia in response to the illegal annexation of Crimea, the FBI began to warn U.S. companies and universities about the risks of entering into technology-sharing agreements with a Russian government-owned firm.[282] Although most of Rusnano's and other similar Russian companies' activities are not connected to intelligence collection, these firms serve as a platform for identifying people and promising technologies that Russian intelligence services can target.

U.S. law enforcement agencies more recently have publicized a steady stream of incidents involving Russian citizens or émigrés illegally exporting or stealing high-tech components or information. In October 2016, the U.S. Government arrested a naturalized U.S. citizen from Russia and two Russian citizens for illegally exporting controlled cutting-edge microelectronics technology from the United States to Russia. The Russians used front companies to purchase the components from U.S.-based suppliers and then falsely classified them on export documents, first shipping them to Finland and then forwarding them to Russia.[283] In another case, several Russians were sentenced in a U.S. court in 2016 and 2017 for establishing front companies in the United States that used false end user certificates to ship approximately $50 million worth of microelectronics components to Russia between 2002 and 2012. The components included analog-to-digital converters, static random-access memory chips, microcontrollers and microprocessors, and other technologies. During the investigation, law enforcement agencies found documents showing orders originating directly from the Russian Ministry of Defense and the FSB.[284]

In July 2018, a Russian father and son, both named Aleksandr Brazhnikov, were indicted in a U.S. federal court for procuring electronic components in the United States and shipping them to Russia. The son owned a U.S.-based electronics export company that advertised itself as offering convenient and inexpensive access to American-made electronics.[285] According to the U.S. indictment, the younger Brazhnikov purchased electronic components from U.S.-based distributors and re-packaged them for shipment to his father in Moscow, falsifying the end users and value of the components. The indictment identified the Russian clients, including the Ministry of Defense, the FSB, and Russian entities involved in the design of nuclear warheads and other weapons.[286]

A more recent arrest in Sweden demonstrated a classic human intelligence method for collecting sensitive technological information. In February 2019, Swedish police arrested a naturalized Swedish citizen meeting with a Russian diplomat, who used the name Yevgeniy Umerenko. The Swedish Foreign Ministry identified Umerenko as an SVR Line X officer responsible for technology collection. Kristian Dmitrievski, the Swedish citizen who had previously held a Russian passport, was described as a specialist in computer simulation and biophysics. Umerenko had been developing Dmitrievski as a source since at least 2017, and Umerenko had previously been observed running similar operations in Germany.[287]

Acting on a U.S. arrest warrant in August 2019, Italian police arrested a Russian citizen, Aleksandr Korshunov, for allegedly using a method similar to what the National Counterintelligence Center in 1995 called "tasking employees of foreign firms." The head of business development for the Russian company United Engine Corporation (UEC), a subsidiary of the Russian state technology conglomerate Rostec, Korshunov was accused of working with Italian citizen Maurizio Paolo Bianchi, the former director of the Italian company Avio Spa, to steal trade secrets; the Italian firm is a subsidiary of the U.S. company General Electric Aviation, which manufactures components for civil and military aviation. Although Bianchi left Avio Spa in 2013, he maintained relationships with several employees, whom he hired as consultants while they were still working for Avio Spa. Bianchi, on Korshunov's instructions, tasked the employees to provide proprietary engineering data about aircraft engines.[288] Both Korshunov and Bianchi were arrested in 2019 and are being held in Italy pending a ruling on extradition to the United States. President Putin personally weighed in on the arrest, claiming that it was based on nothing but the United States trying to eliminate the competition.[289] In a blatant attempt to derail the extradition, the Russian government demanded that Korshunov be extradited not to the United States, but to Russia on a suddenly emerging embezzlement charge; Putin did not mention the embezzlement charge in his statement.[290]

Similar to the operations that prompted the 1982 U.S. National Intelligence Council assessment of Soviet technology collection, these cases demonstrate several collection methods—from classic human intelligence recruitment in Sweden to establishing front companies in the United States and entering into a consultant relationship with employees of a competing company in Italy. They also show Russia's sense of urgency to overcome sanctions-related barriers that inhibit its technological development, especially for technology that has military and security applications.

This technological intelligence activity reveals, however, another weakness in the Russian, and in its predecessor Soviet, economic system. The centrally managed Russian economic system itself inhibits the technological innovation that freer political and economic structures encourage. The Russian government, not private research organizations or companies, funds the majority of S&T research, which both limits the funding available for basic research and focuses it on government priorities, particularly defense priorities. Additionally, many educated Russians would prefer to emigrate from Russia for better economic opportunities abroad, creating a brain drain effect that inhibits Russian high technology research.

Consequently, Russian intelligence services are dispatched across the world to steal what Russia cannot develop domestically. Russia's innovation ecosystem cannot support many of the technology development needs that the Russian government has identified as priorities, such as artificial intelligence and automation. By applying its intelligence services to these hard-to-develop technologies, Russia is essentially outsourcing its innovation. That dynamic is self-defeating in the long term, because a national program to steal technology effectively ties the Russian economy to innovations developed in other countries rather than producing its own. Thus, Russia's use of intelligence capabilities to advance its aspiration to become a great power—and the systemic weakness it demonstrates—serves to condemn Russia to permanent second-class status as a scientific and technological power, notwithstanding its intelligence successes.[291]

Just as the KGB boasted of having recruited sources in IBM, Texas Instruments, ITT, and the National Institutes of Health, Russian intelligence tries to do so in equivalent enterprises around the world today for the same reason. While that intelligence collection can damage the national security of the countries from which technology and technical know-how is stolen, it may not provide Russia with the long-term benefit it hopes for itself.

ECONOMIC INTELLIGENCE

Economic intelligence is the collection of information on foreign governments' economic activities, economic and financial organizations, raw materials markets, metals, and currency, which are priorities for the Russian Federation. Russian economic intelligence includes supporting institutions that create favorable conditions for Russia to achieve its foreign economic objectives and targeting foreign countries' economic actions that disadvantage Russia.

The SVR is the primary organization responsible for economic intelligence, and several SVR elements have related responsibilities. The SVR directorate dedicated to this type of collection is *Экономическая Разведка* (Directorate ER). Directorate NTR also plays a role. Additionally, separate from both Directorate ER and Directorate NTR, a third directorate manages what are called "measures of support," or what during the Soviet era were called "active measures." These measures of support involve disinformation operations that are intended to influence a foreign power to act in a way that is beneficial to Russia, and they occasionally facilitate the work of the economic and S&T directorates. In a recent case, intelligence collected by an SVR officer under nonofficial cover fueled a Russian influence operation to gain Canadian support for an aircraft manufacturing joint venture, highlighting this connection (see below).

Retired SVR officer Sergey Vorontsov defines economic intelligence as

> Receiving information on all fields of foreign political actors' economic activity and their economic and financial structures, currency market conditions, raw materials, precious metals, etc., that are of interest to Russia, and also the organization and management of enterprises directed toward creating profitable circumstances for Russian foreign economic interests, for developing effective foreign economic cooperation, concluding profitable trade and economic deals and agreements, etc.[292]

Russia requires the economic intelligence that Vorontsov describes to give its struggling economy a boost in an interconnected economic world. Just as with S&T collection, there are many economic fields in which Russia legitimately interacts in the global economic environment. However, global economic interconnectedness is itself a threat to Russia's strength because of the cutthroat world of economic competition. Thus, in addition to Vorontsov's traditional definition, much of Russia's "economic intelligence" is related not just to studying other countries' economic systems per se, but also to collecting intelligence about efforts by perceived adversaries to harm Russia's economy, operating on the foundational assumption that such a phenomenon is invariably occurring. Soviet/Russian intelligence services have a long history of collecting information about real or presumed unfriendly foreign power activities to "wreck" the Soviet/Russian economy. This activity also enters into the category of economic counterintelligence, which will be discussed in the next section of this chapter.

Soviet Era

The Soviet Union operated on the ideological assumption that capitalist countries were bent on destroying the Soviet economy. Suspicions of the West, fueled by a mixture of anti-capitalist dogma and a sense of economic inferiority, drove the Soviet Union to apply its intelligence collection capabilities to protect it from what it viewed as a hostile global environment. The Soviet Union regularly conducted intelligence operations to circumvent the perceived anti-Soviet commercial practices of foreign countries. Orlov claimed that the Soviet Union believed foreign companies colluded to raise the prices of their exports to Russia 60 to 75 percent to bilk the Soviet Union and to take advantage of Russia's poor credit rating.[293] Consequently, Soviet state security was charged with controlling Soviet export and import operations and protecting Soviet foreign trade from perceived pressures and abuses from international cartels and other organizations of monopolistic capital.[294]

Based on those suspicions, Soviet illegal Ignatiy Poretskiy (aka Ignace Reiss) operated in Germany during the 1930s under nonofficial cover as a Soviet Planning Committee (GOSPLAN) specialist and journalist. His cover provided him access to German economic information and was sufficiently convincing to fool a British intelligence source who encountered Poretskiy/Reiss in 1933 and assumed that he had left intelligence work altogether and joined the GOSPLAN full time. As the source reported, Poretskiy/Reiss was formulating a variety of economic projects.[295]

Similarly, Soviet illegal Iosif Volodarsky, mentioned earlier in relation to S&T collection, worked undercover as an employee of the Soviet company, Russian Oil Products, in the United Kingdom before his assignment to the United States. He was arrested in London in 1932 for trying to recruit a British oil company employee to provide proprietary information about the company's production and sales figures. Volodarsky's requests came just after the Soviet Union had lost a contract for supplying petrochemical products for the British military.[296]

During Stalin's reign, Soviet leaders preached the threat of capitalist encirclement, which they used as a pretext to explain poor Soviet economic performance. One former NKVD officer wrote that his supervisors gathered office personnel together to explain why there were long lines for consumer goods. They claimed that the problem was international capitalism and that an unnamed saboteur, using money from foreign capitalists, was buying up all of the goods manufactured for the Soviet people, creating shortages in the Soviet Union. The solution was a more serious study of Communist Party history and theory.[297] Capitalist encirclement continued to drive Soviet thinking after World War II and throughout Stalin's reign.[298] Although today the Cold War-era communist ideology is stripped away from Russian thinking, Russian propaganda still claims that the United States is pursuing a policy of "hostile encirclement" of Russia.[299] Similar to during the Soviet era, the answer today is Russian patriotic education, accompanied by economic intelligence efforts to reveal the adversarial plans of the United States and other economic powers.

Soviet economic intelligence operations went beyond collecting intelligence to include actively manipulating and undermining capitalist countries' economies. Petr Karpov, an OGPU officer who defected in Germany in 1924, claimed that the Soviet government, via OGPU clandestine operations, attempted to disrupt foreign economies by disseminating counterfeit foreign currency.[300] Ginzberg/Krivitsky later wrote about a Soviet operation to counterfeit U.S. currency, which he described as an attempt by Stalin to add hard currency to the Soviet treasury.[301] The operation resulted in arrests of OGPU agents in Germany in 1929 and in the United States in 1933 after police found counterfeit currency originating from the Soviet Union.[302] Orlov was in Germany when the story broke about counterfeit U.S. banknotes being deposited in a German bank, forcing him to flee in the face of intensified German counterintelligence scrutiny.[303]

Post-Cold War

Although no longer fueled by the communist-capitalist ideological conflict, Russia's suspicions about foreign government intent continue in the 21st century. The 2015 arrest of Yevgeniy Buryakov, an SVR officer working under nonofficial cover in the New York City office of the Russian bank VneshEconomBank, and two Russian diplomatically covered SVR officers, Igor Sporyshev and Viktor Podobniy, demonstrated the continuing application of intelligence resources toward this line of effort. The operation revealed requests from Moscow for intelligence on economic issues, including potential U.S. sanctions against Russia and U.S. efforts to develop alternative energy resources.[304] Russian officials interpret sanctions as evidence that the West, especially the United States, is intent on destroying Russia's economy.

Buryakov arrived in the United States in August 2010 and began using his position in banking circles to support Russian intelligence collection activities. In 2013, Sporyshev tasked Buryakov to help formulate questions that a Russian ITAR-TASS news agency journalist could use for intelligence collection. Buryakov recommended the following questions, as subsequently recorded in the U.S. Department of Justice indictment:

- Ask about how the New York Stock Exchange uses exchange-traded funds, particularly how they are used as mechanisms for destabilization of markets.
- Ask them what they think about limiting the use of trading robots.
- Ask about technical banking matters involving the exchange of funds to the Russian Federation, such as "technical parameters" and "other regulations directly related to the exchange."[305]

A few weeks later, an SVR officer operating undercover as an ITAR-TASS journalist sent an email to an employee of the New York Stock Exchange repeating Buryakov's proposed questions nearly verbatim.[306]

As early as April 2014, shortly after the international community imposed economic sanctions on Russia, Sporyshev relayed collection tasking to Buryakov to research "the effect of economic sanctions... on our country." In response, Buryakov conducted Internet searches for "sanctions Russia consiquences [*sic*]" and "sanctions Russia impact" and reported the results to Sporyshev.[307] In mid-2014, Buryakov also began cultivating an American businessman who offered information about U.S. sanctions. The source, who unbeknownst to Buryakov was cooperating with the FBI, approached Buryakov with a proposal to establish a casino in Russia. In the course of his presentation, the source remarked about the impact of sanctions on the proposed project, and he produced a document labeled "Internal Treasury Use Only" that contained a list of Russian individuals subject to U.S. sanctions. The source asked whether Buryakov was interested in such information, to which Buryakov responded enthusiastically and asked to take the document with him. The source later showed Buryakov a list of Russian banks, marked "UNCLASSIFIED/FOUO," and told him that the U.S. Government used the list to identify Russian banks on which to impose sanctions. Buryakov expressed interest in getting more information about sanctions, specifically information about when additional sanctions would be imposed, the types of sanctions, and on which companies or entities. He tasked the source to provide information not just about banks, but about any Russian institution that could be affected by sanctions.[308]

Buryakov's mission also included supporting an influence operation—or "measures of support"—to remove obstacles to a huge Russian trade deal. In 2012 and 2013, the Russian aircraft technology company Rostec—the same company involved in a 2019 arrest in Italy noted above—was in negotiations with the Canadian aircraft manufacturer Bombardier to create a multimillion dollar joint venture that would allow Rostec to manufacture Bombardier's Q400 aircraft in Russia.[309] However, Canadian labor unions associated with Bombardier opposed the plan, fearing the loss of jobs.[310] The SVR's solution was to launch an influence operation geared toward pressuring labor unions to drop their opposition and approve a deal on Russia's terms. Buryakov's role was to travel to Canada several times and gather information to feed that influence operation.[311] The deal started to break down when the West imposed sanctions on Russia; Bombardier pulled out of the deal altogether in late 2014, rendering the proposed influence operation moot.[312] Nevertheless, the FBI investigation of Buryakov from 2012 to 2015 provided evidence that Russia continued to task its intelligence services to collect economic intelligence and to influence foreign economic decisions, as it had done during the Soviet era.

In a separate case, a bank employee was the target of an alleged Russian intelligence operation in Japan. This Japanese SoftBank employee was arrested in January 2020 for passing confidential bank information to Russian officers covered as employees at the Russian Trade Representation in Tokyo beginning as early as 2017. The arrested employee admitted to stealing low-level information. Nevertheless, the Russian Embassy provided a typically reflexive response, claiming that Russia "regrets Japan has joined anti-Russian speculation trend in the West on the hackneyed topic of spy mania."[313]

Russia's actions to overcome sanctions also benefit its allies. In some cases, Russia-affiliated companies use their vast sanctions-busting experience to support Russian allies that are encountering similar obstacles, such as Zimbabwe, Iran, and Syria. A U.S. citizen was arrested in 2010 for selling Russian helicopters to Zimbabwe in violation of sanctions; the purchase was made through a Russian company.[314] A naturalized U.S. citizen from Iran was arrested in 2013 in the United States for acquiring technology that helped Iran launch its first earth imagery reconnaissance satellite; the satellite was launched in partnership with the Russian government.[315] In June 2018, eight businessmen, including five Russian nationals who worked for the Russian shipping company Sovfracht and three Syrian nationals, were indicted in a U.S. federal court for conspiring to send jet fuel to Syria and for conducting U.S. dollar wire transfers to Syria in violation of U.S. economic sanctions against Syria and Crimea. After the U.S. Government placed sanctions on Sovfracht, the Russian employees created a front company to conduct the money transfers and deliver the fuel to Syria with less scrutiny.[316]

As oil is such a significant element of the Russian economy, Russian illicit activity in the oil market is especially prominent, reportedly with intelligence service support. Russian SVR defector Sergey Tretyakov revealed the SVR's involvement in running the UN Oil-for-Food program in the late 1990s, which allowed Iraq to sell oil vouchers for food imports into Iraq. According to Tretyakov, an SVR Directorate ER officer was assigned undercover to the UN office responsible for administering the Oil-for-Food program. The SVR officer eventually became the sole administrator of the program, allowing him to manipulate prices and give senior Russian government officials and other Russian entities, including the Russian Presidential Administration, as well as other people who were friendly to Russia, opportunities for enormous profits as they traded on the vouchers.[317] This same sort of operation may have a more recent analogue: in 2015, the EU placed sanctions on George Haswani, based on what the EU called overwhelming evidence that he was serving as a middleman for oil purchases by the Syrian regime from the so-called Islamic State.[318] The U.S. Government designated Haswani for sanctions later the same year.[319] According to Turkish media, Haswani is a dual Russian-Syrian citizen who was trained in Russia.[320] Although SVR involvement in the Haswani allegation is not firmly established, the case resembles the SVR's illicit activity in the 1990s.

With SVR intelligence support, the Russian government backs the Russian oil and gas industry, while undermining other countries' competing industries. If reports are true that the director of Russia's state oil company Rosneft, Igor Sechin, is a former KGB officer, this association may influence that SVR support.[321] According to a U.S. intelligence assessment, the Russian government conducted an aggressive propaganda campaign to criticize the natural gas extraction method known as fracking, probably driven largely by the Russian government's concern about the impact of U.S. natural gas production on the global energy market and its potential challenges to Russia's profitability.[322] Possibly connected to this, alternative energy sources were revealed as intelligence targets in the FBI investigation of Yevgeniy Buryakov. Igor Sporyshev, an SVR officer who worked with Buryakov, began cultivating a U.S. oil industry expert in 2013, promising him access to oil deals in Russia in return for information about the oil and gas industry. An SVR officer at the time explained his recruitment method, which included cheating, promising favors, and then discarding the intelligence source once the SVR obtained the relevant information.[323]

Other countries' oil and gas infrastructure is another frequent target of Russian collection. In April 2019, Lithuanian police arrested a Russian-born Lithuanian citizen, Romanas Šešelis, for providing information about the LNG terminal operator Klaipėdos Nafta and other infrastructure to a Russian intelligence agency between 2015 and 2017.[324] Based on unconfirmed allegations, individuals involved in the Nord Stream II pipeline project—designed to transport Russian natural gas to the EU—may also have Russian intelligence connections. Suspected individuals include Nord Stream CEO Matthias Warnig, an ex-captain in the East German Stasi, who is now closely associated with President Putin, himself an ex-KGB officer who served in East Germany.[325] U.S. intelligence officials have also voiced suspicions that the intelligence relationship to the petrochemical industry could go the other direction, expressing concerns in 2018 that the Nord Stream pipeline system could allow Moscow to emplace listening and monitoring technology on the Baltic seafloor.[326]

The close connection that ties the Russian economy, especially the oil and gas industry, to Russian national security drives Russia to apply its national security apparatus, including its intelligence capabilities, to monitor economic developments worldwide. Economic intelligence collection and influence operations both protect against suspected foreign efforts to damage the Russian economy and undermine economic competition.

ECONOMIC COUNTERINTELLIGENCE

The third application of Russian intelligence and state security in the economic arena is economic counterintelligence. This is the mechanism by which the Soviet, and now Russian, government has used economic levers internally to prevent damage to the ruling regime, whether it be the Bolshevik regime of the early post-revolutionary period or the Putin regime today. The objectives and methods have remained similar across the 100-plus years since the Bolshevik revolution. Economic counterintelligence is weighted more heavily toward state security than intelligence. Nevertheless, it uses various clandestine means to accomplish its missions. Economic counterintelligence has two primary directions: to prevent the leakage of Russian economic information abroad, even information that most countries publish openly, and to use economic levers to punish antiregime activists at home.

Today, economic counterintelligence is the FSB's responsibility through its dedicated Economic Counterintelligence Service, which is responsible for monitoring the credit and financial, industrial, telecommunications, and transportation sectors of the Russian economy. Within the Economic Counterintelligence Service are three primary operational departments:

- Department K, which provides counterintelligence services for banks and financial institutions.
- Department T, which provides counterintelligence services for the transportation sector.
- Department P, which provides counterintelligence services for industrial enterprises.

The Economic Counterintelligence Service's functions differ from economic intelligence and S&T intelligence because they are derived from the Soviet-era KGB Second Chief Directorate, which was responsible for internal counterintelligence, as well as the KGB Fourth and Sixth Directorates, which had counterintelligence responsibilities in the economy. Consequently, these functions operate separately from the SVR and GRU foreign collection operations.

Soviet Era

Immediately after the Bolshevik revolution, the regime had an urgent need to stabilize the internal economic situation. Less than a year after the revolution, new missions were added to the first Bolshevik state security organization, as evidenced by its name's expansion: the All-Russian Extraordinary Commission for Combating Counterrevolution, ***Profiteering, and Corruption*** (VChK) (emphasis added). Corruption among Soviet officials had reached the severity of a national security threat.

Several intelligence officer defectors who had been involved with Soviet state security in its earliest days have provided insights into this economic side of state security. Orlov, writing under the pseudonym Lev Nikolayev, published several articles in the journal *Soviet Justice Weekly* in 1923 exposing the financial misdemeanors of Soviet officials. In one case, he wrote about a judge collaborating with a prosecutor to demand bribes for leniency—the accused were convicted and sentenced to execution.[327] In another case, a prosecutor offered freedom to a suspect on the condition that the family pay 500 million rubles.[328]

OGPU defector Petr Karpov noted that economic crime was integrated into the Soviet state security service from its foundation. He wrote that the VChK could not meet all of its operational expenses with official allocations from the Bolshevik government. Consequently, the VChK was forced to supplement its income by selling property requisitioned from wealthy Russian citizens, trafficking contraband goods confiscated in raids, and counterfeiting tsarist-era currency. But eventually, this authorized criminal activity had to be brought under control, and the Soviet state security service was forced to pursue its own people for economic crimes.[329]

Corruption and domestic economic resistance remained a state security concern through the rest of the Soviet era. As Stalin ordered the collectivization of farms, those who resisted were labeled "wreckers," and anyone who refused to fulfill state orders was accused of economic "sabotage."[330] The NKVD Economic Department was the preeminent state security element of the early 1930s, as the Soviet Union was striving to establish its industrial base and collectivize agriculture, according to KGB defector Petr Deryabin.[331]

During the Soviet era, people viewed as traitors were often accused of committing economic crimes. When a Soviet embassy learned of a defection, it reflexively claimed that the defector had stolen or embezzled money, and thus should be returned to face Soviet criminal charges. For example, when Lithuanian merchant seaman Simas Kudirka attempted to defect to a U.S. ship in 1970, the immediate response from Soviet authorities was that Kudirka had stolen 3,000 rubles from his Soviet ship's safe and thus should be returned as a fugitive criminal.[332] Vladislav Krasnov, in his groundbreaking 1985 book on Soviet defectors, noted that stealing money or property was the most common accusation Soviet authorities made when demanding the return of a defector. However, official Soviet court indictments against defectors included theft in only a small percentage of cases, indicating that the claim of an economic crime was usually only a superficial attempt to besmirch the defector's name and demand extradition.[333] As was pointed out in a U.S. Congressional hearing following the Kudirka incident, "it seems fairly obvious that anyone who was going to defect would not steal rubles. That would be excess baggage."[334]

Additionally, as noted above in relation to economic intelligence, the Soviet Union routinely expected capitalist powers to overcharge and cheat Soviet purchasers, so it employed economic counterintelligence measures to circumvent disadvantageous deals. In 1936, for example, Iosif Volodarskiy purchased shares with NKVD money in a New York City company called Round the World Trading Company. Based on the assumption that Western trade partners colluded to overcharge and bilk the Soviet Union, Soviet intelligence used this company to gather commercial information.[335] When the Soviet Amtorg Trading Company sent an offer to an American firm to purchase machinery, Volodarskiy, using the American-based Round the World Trading Company as cover, contacted the same American suppliers and asked for price quotations for the same products. Amtorg could then compare prices and determine whether it was being overcharged as a Soviet entity.[336]

Post-Cold War

Today, the Russian government, particularly the FSB, uses the enforcement of economic crime laws as a lever to inhibit the activities of foreign powers and domestic opposition groups inside Russia. Additionally, Russian national security leaders have expressed a suspicion similar to Soviet-era leaders, that foreign powers are intent on destroying the Russian economy. For Russia, counterintelligence is not narrowly defined as catching spies, but it also includes preventing anyone, whether foreign or domestic, from countering the regime's power. That reasoning extends into the economic realm.

Foreign nongovernment organizations (NGOs) that support Russian democratic civic groups are a particular target of Russian accusations of foreign economic intrigue. In 2004, President Putin accused Russian NGOs of pursuing "dubious group and commercial interests" for taking foreign money. FSB Director Nikolai Patrushev told the Russian State Duma in 2005 that the FSB had uncovered spies working in foreign-sponsored NGOs. He further claimed, "Foreign secret services are ever more actively using non-traditional methods for their work and, with the help of different NGOs' educational programs, are propagandizing their interests, particularly in the former Soviet Union." Patrushev accused the United States of placing spies undercover within the Peace Corps, which was expelled from Russia in 2002, the Saudi Red Crescent, and the Kuwaiti NGO Society for Social Reform. Patrushev attributed an economic motive to these perceived foreign plots, alleging that industrialized states did not want "a powerful economic competitor like Russia." Echoing Soviet-era accusations of nefarious Western economic intent, he claimed that Russia had lost billions of dollars per year due to U.S., EU, and Canadian "trade discrimination."[337] Pushing for stronger regulation of NGOs, Patrushev said, "The imperfectness of legislation and lack of efficient mechanisms for state oversight creates a fertile ground for conducting intelligence operations under the guise of charity and other activities."[338] In 2012, Putin signed the "foreign agent law," which ordered Russian civil rights organizations that received any foreign funding to register as "foreign agents."[339]

The FSB also regularly uses economic statutes to suppress political forces that rival Russian central authority and facilitate infighting among rival elites. Through a number of high-profile arrests, this FSB tactic has become one of the foremost manifestations of economic counterintelligence within Russia. In some cases, arrests have silenced criticism of official corruption within the government itself.

Mikhail Khodorkovsky, an oligarch who used dubious commercial practices to become the richest man in Russia during Boris Yeltsin's time as president, clashed with Putin and was arrested in 2003, along with other executives of the oil giant Yukos, for tax evasion and economic crimes. Although he was certainly not the only oligarch whose wealth was founded on a questionable basis, his primary offense was his support for politicians who opposed Putin. Khodorkovsky was sentenced in 2005 to nine years in prison. He was charged with other economic crimes while serving his sentence, and he was finally released in 2013 and left Russia.[340] In May 2020, an organization sponsored by Khodorkovsky published an online expose on the FSB, titled *The Lubyanka Federation*, that highlighted the agency's economic focus, showing that the allegations against him have not silenced him.[341]

In another case, American-British investor William Browder became infamous in Russia for his claims of Russian government corruption. In 2008, Browder's Moscow-based tax advisor, Sergey Magnitsky, alleged that Russian police and tax authorities had attempted to steal over $200 million from the company, claiming that it was delinquent in its taxes. The case was widely seen as retaliation for Browder's anti-corruption campaign, and Magnitsky was arrested after publicizing the allegation. Magnitsky later died in prison, inspiring the United States to institute the Magnitsky Act, which levies sanctions against corrupt Russian government officials.[342] Magnitsky was later tried posthumously in Russia for tax fraud.[343]

One of the highest profile arrests based on an alleged violation of a financial statute came in 2016, when the FSB arrested Russian Minister of Economy Alexei Ulyukayev. He was accused of trying to extort $2 million from the oil conglomerate Rosneft to approve its purchase of the state-owned oil company Bashneft. The case has been assessed as the result of infighting within the power centers of the Russian government. Rosneft director and Putin loyalist Igor Sechin, an economic hard-liner, reportedly launched the bribery accusation against Ulyukayev, an economic liberal. Ulyukayev was sentenced to eight years in prison in 2017.[344]

Similarly, anti-corruption activist Aleksey Navalny was arrested in 2013 on embezzlement charges. His case was dismissed but retried in 2017, when he was found guilty. The guilty verdict effectively barred him from running in the 2018 presidential election and, thus, the allegation of economic malfeasance removed a potential political opponent to Putin.[345] Amid these actions, the Russian State Duma passed legislation that would make it illegal for a Russian citizen to reveal any Russian-government information without explicit approval, thereby blocking foreign government investigations into fraud or corruption by Russian subsidiaries of multinational corporations.[346] The new law also made it illegal to publish statistics of the Russian economy independently of the Russian government itself.

The FSB's economic counterintelligence role has also arisen as a lucrative way for FSB officers to get very rich, echoing the early days of Bolshevik state security. The Soviet, and now Russian, security services' use of economic criminal procedures—simultaneously to protect the ruling regime and to silence anyone who criticizes regime-sponsored corruption—has been a continuous characteristic of economic counterintelligence since the earliest days of the Bolshevik regime. Regime-sponsored corruption is far from a thing of the past. Just as the VChK did in the early Bolshevik period, FSB investigators today use counterintelligence powers to capture vast amounts of money. Oleg Vyugin, a former senior official at the Bank of Russia and the Ministry of Finance, went so far as to say that the security services have "become one of the key elements of the economy... Unfortunately, they're an element that's an obstacle to its normal development."[347]

FSB Colonel Kirill Cherkalin was arrested in May 2019 with money and valuables totaling over $180 million in his apartment. Two other FSB officers, Dmitry Frolov and Andrey Vasilyev, were arrested soon after that. Cherkalin had been a manager in Department K, the FSB component responsible for economic counterintelligence in the banking sector, and he was reportedly a member of an interministerial committee for fighting money laundering, terrorism financing, and proliferation of weapons of mass destruction;[348] FSB Department K had investigated Sergey Magnitsky in 2008 and Aleksey Navalny in 2013. Cherkalin was accused of using his regulatory power over banks to demand bribes and protection money. The *Moscow Times* reported after Cherkalin's arrest that FSB officers could extort money from banks in several ways: they could demand a percentage of all cash withdrawals (up to 0.2 percent of the transactions), or they could demand bribes and payoffs for specific violations.[349] In November 2020, a former FSB Department K officer Aleksey Artamonov (aka Janosh Neumann) claimed that money laundering has become so rampant in Russia that the authorities responsible for combating it cannot defeat it, so they have decided simply to control it; however, staying "clean" is impossible when FSB officers are involved in state-supported money laundering operations.[350]

Because money laundering is common in Russian banks, Russian bank regulators can readily claim grounds for pressing their corrupt demands. The Ministry of Interior faces the same temptation. In October 2019, a Moscow court sentenced a colonel from a Ministry of Interior department responsible for regulating banks to 12 years in prison for bribery and obstructing justice; the colonel had accumulated more than $125 million in bribe money.[351] Orlov's articles about official corruption in the 1920s do not appear as distant as time would suggest.

METHODS AND MOTIVATIONS IN THE ECONOMIC AND S&T REALM

Available information shows that Russian services heavily rely on human methods, such as agent recruitment, front companies, and human penetrations of competing companies, for economic and S&T intelligence tasks. Russia has also taken advantage of a foreign corporate environment that is willing to cooperate with Russian companies, using corporate agreements and investments as platforms for intelligence activities. Some of these deals have also become the target of Russian disinformation campaigns when there is a threat that things might not go Russia's way. Russian intelligence officers also collect open-source information clandestinely or task sources to collect information for them.

As Russian computer-based intelligence activities have been widely publicized over the past several years—centering primarily on aggressive Russian actions against geopolitical adversaries, such as Ukraine, the United States, and Western European countries—reports have increased of these same methods being used for economic and technological collection. For example, in 2011, the U.S. Office of the National Counterintelligence Executive changed the name of its annual report to Congress from *Economic Collection and Industrial Espionage* to *Foreign Spies Stealing U.S. Economic Secrets* *in Cyberspace*.[352] In 2018, that same organization repeated this theme in a report titled *Foreign Economic Espionage in Cyberspace*.[353]

Publicly available information, however, provides a less compelling argument that Russia uses computer-network operations as a primary method for collecting economic and technological information, although it does extensively use computer-based operations for internal economic counterintelligence purposes. For foreign targets, Russian computer network threat actors appear instead to be more focused on fulfilling Russia's military and political requirements. Even in cases where a Russian actor targets an industrial enterprise, the actions often appear to be for sabotage rather than intelligence collection.

Only a handful of the reported Russia-related incidents in the Council on Foreign Relations (CFR) database of government-sponsored computer intrusions noted in Chapter 4 appear to have an economic or technology collection motive, and even those are mixed with geopolitics. In late 2016, a computer-network threat actor, believed to be affiliated with Russia, targeted Ukrainian banks and destroyed banking data, and, in early 2017, a threat actor targeted infrastructure entities in the oil and gas sector, primarily in Ukraine. A threat actor targeted biological and chemical laboratories in Ukraine and other countries in Europe in mid-2018, probably in reaction to allegations of Russia's use of a chemical agent in the Sergey Skripal assassination attempt in the United Kingdom. Later in 2018, a threat actor targeted U.S.-based Westinghouse Electric Company, a nuclear power developer. None of these activities appear to be solely to collect economic or technological information for Russian exploitation, but instead to have the primary mission of collecting information that could be used for geopolitical confrontation purposes, particularly in relation to Russia's aggressive actions against Ukraine.

The CFR's database is by no means comprehensive. CFR relies solely on information that is publicly reported, and its data collection emphasizes politically driven operations. Nevertheless, this database seems to align with the analysis of other organizations that monitor Russian-sponsored computer network attacks. For example, the computer security company FireEye concluded in 2014 that the activities of the widely known Russian-based group labeled APT28 (aka Fancy Bear), which the U.S. Department of Justice assessed was affiliated with the GRU, indicated a political, not an economic motive.[354] According to FireEye, "this group, unlike the China-based threat actors we track, does not appear to conduct widespread intellectual property theft for economic gain. Nor have we observed the group steal and profit from financial account information." APT28's activities suggest more a motive to collect intelligence on Russian defense and geopolitical interests rather than economic interests.[355]

Another Russian computer network threat group, APT29 (aka Cozy Bear) also targets political information. The Dutch intelligence service AIVD has assessed that APT29 is affiliated with the SVR or the FSB,[356] and U.S. investigators have connected APT29 to the SVR after the 2020 SolarWinds operation.[357] Primary targets for another Russian threat group labeled Venomous Bear (aka Turla) are in the government, aerospace, NGO, defense, cryptology, and education sectors. Venomous Bear, possibly sponsored by the FSB, was particularly active in early to mid-2015 when it compromised multiple countries' embassy, government, educational, and NGO websites.[358]

One Russian computer network threat group appears to be more focused on economic targets than the others. Energetic Bear has targeted industrial control software vendors, potentially giving hackers access to everything from power grid systems to manufacturing plants. The group seemed at least in part focused on broad surveillance of the oil and gas industry, including gas producers, firms that transport liquid natural gas and oil, and energy financing companies.[359] In the context of Russia's intelligence activities, this may fall into the economic intelligence category, since foreign oil and energy companies compete with Russian companies in the global petrochemical market.

The U.S. Defense Counterintelligence and Security Agency's 2019 report mentioned above indicates that only 17 percent of reported incidents of foreign targeting of U.S. cleared defense contractors have been conducted via computer-based operations. These attempts usually come in the form of unsolicited emails carrying malicious code, which computer security protocols often catch.[360] With some technologies, like electronics and aeronautics, which were noted above as being the targets of human-based operations, computer network operations are even less prevalent.[361]

Nevertheless, the German Federal Office for the Protection of the Constitution reported in 2016 that a GRU-affiliated hacking campaign was observed operating in German research institutions and companies, especially in the field of laser technology and optics.[362] More recently, Russian computer-based intelligence collection operations may have targeted pharmaceutical companies in the race to find a vaccine for COVID-19.[363] Russian leaders made public statements in 2020 encouraging Russian companies to be the first to find a vaccine, because it would bolster Russia's technological reputation in the world. Even in this case, Russia has a geopolitical motive for its intelligence collection operation, not merely an economic one.

The U.S. National Counterintelligence and Security Center's (NCSC's) 2018 report, *Foreign Economic Espionage in Cyberspace*, claimed that "in recent years Russia has dramatically increased its demand for source code reviews for foreign technology being sold inside the country."[364] The NCSC interprets these actions as being related to economic collection. That may be valid, inasmuch as Russia relies on Western technology to maintain its economy, as noted earlier. However, such a trend could just as easily fall within the FSB's economic counterintelligence mission. Founded on Russia's historical suspicion toward foreign powers and the assumption that they are invariably trying to damage Russia's economic potential—along with the reality that the FSB, the entity responsible for economic counterintelligence, conducts most of these code reviews—it should come as no surprise that Russia might use these source code reviews to protect Russia's economic and defense sectors from perceived foreign enemies or internal threats.

The NCSC's 2018 report also assessed that "Russia uses cyber operations as an instrument of intelligence collection to inform its decisionmaking and benefit its economic interests." In support of that assertion, NCSC cited a claim by a Russian hacker, who used the handle "Eas7" and in 2016 reported having collaborated with the FSB on economic espionage missions.[365] Eas7 is probably Alisa Belousova, a 2004 graduate of the North Caucasus State Technical University who has described herself as a programmer, system administrator, computer security analyst, and system architect.[366] NCSC did not mention in its analysis that the report about "Eas7" originated with a 2016 article in the online tabloid site *Vice TV*. Although that report has been repeated online, it has not been corroborated.[367] The remainder of the examples that NCSC provides in its 2018 report are more likely related to either political collection or critical infrastructure collection supporting military contingency planning (see Chapters 4 and 7, respectively).

CONCLUSION: NATIONAL SECURITY CONCERNS FUEL ECONOMIC/S&T COLLECTION

Economic and S&T collection are potent tools for the Russian government to use in maintaining and growing its economic and military strength. Because Russia's economic status, especially as it relates to oil and gas commodities, plays such a pivotal role in Russia's national security decisionmaking, Russia feels an urgent need to understand foreign economic plans and technological developments. Such collection starts from the foundational assumption that Russia is surrounded by adversarial powers, which is reinforced by sanctions designed to change Russia's inimical geopolitical behavior. Unlike in political intelligence collection, where computer-based methods have become increasingly prevalent, as evidenced by the SolarWinds operation in 2020, human operations still predominate in foreign economic and S&T collection. Inside Russia, however, where the Russian government enjoys nearly complete control over the telecommunications environment, the FSB and other Russian services heavily use computer surveillance and other technical methods to monitor the domestic oppositionist activities—and these investigations often employ economic counterintelligence resources and laws.[368]

CHAPTER 6

MILITARY INTELLIGENCE

As discussed in the previous two chapters, both political and S&T collection contain a defense component that supports political decisionmaking and technological development. Defense-related collection seeks to understand a potential adversary's defense policies and research and development toward future weapons capabilities at the strategic level. Those are important elements of military intelligence.

Another part of military intelligence is to collect the information that military forces will need to conduct military operations, both in a current, tactical context and in a broader, strategic context. There are three main major components of Russian intelligence that support military activity:

- **Foundational military intelligence**, which collects and analyzes information about the basic elements of a foreign military force that the Russian military would face in a military conflict.
- Intelligence on **strategic forces, particularly nuclear weapons capabilities**, and strategic missile defense capabilities, which touch on Russia's primary military capability—its strategic nuclear deterrent.
- Intelligence for **strategic contingency purposes**, which includes collecting intelligence about and planning for future attacks on an

adversary's critical infrastructure that would support military action if Russia ever found itself in a war.

This chapter is organized around these three components. Intelligence collection to support military decisionmaking is primarily the GRU's role, although the SVR, as did the KGB before it, also runs sources who provide military-related information, and the FSB is involved in this collection in the countries of the former Soviet Union.

During the Cold War, the United States gathered a large amount of information about the priorities and targets of Soviet military intelligence, including what the Soviet military wanted to know about the United States and its allies and how the Soviet military acquired that information. A focus on the Cold War still provides valuable lessons for several reasons: first, a large amount of information is publicly available, and second, the GRU is the Russian intelligence organization that has changed the least since the Soviet era. The activities of the Soviet era continue to provide a useful pattern for how Russia conducts military intelligence activities today.

Of the approximately 100 publicly known Soviet intelligence officers who defected or attempted to defect during the Cold War (1945 to 1992), about one-fourth of them were GRU officers. Despite their smaller number these officers provided unique information about all three of the Soviet military intelligence collection directions described above (see also Figure 18).

From 1945 to 1992, at least 11 of the approximately 100 intelligence officers who defected chose to redefect. Of those redefections, six were GRU personnel, making up a much larger proportion of redefectors than of the total defector number. Of those six, four redefected in the early 1970s and three within a three-month period in 1973. The reason for these redefections is unclear, but there are several potential explanations: a deliberate Soviet program to dispatch intelligence officers as defectors and then bring them back for propaganda purposes; a less welcoming resettlement program in the United States; or a group of young Soviet officers who struggled to adapt to a new, foreign environment. More research is needed to determine which of these explanations fits this brief period of redefections.

Figure 18. **GRU Officers Who Defected or Attempted To Defect During the Cold War**

Igor Gouzenko, 1945: GRU taskings to collect U.S., British, and Canadian weapons and troop information

***Name unknown*, 1946:** Radio operator for GRU special-purpose radio unit in Hungary

Vladimir Skripkin, 1947: Diplomatic cover in Japan (failed defection)

Mikhail Denisov, 1947: Interpreter for Allied Control Commission in Hungary and at Soviet embassy in Hungary

Vadim Shelaputin, 1949: GRU translator in Vienna; designated to run operations

***Name unknown*, 1950:** Operational-Intelligence Section of a GRU unit in the Group of Soviet Occupation Forces in Germany

***Name unknown*, 1953:** GRU illegal sent to infiltrate Turkey

Ivan Ovchinnikov, 1956: Translator for 28th Separate Radio Regiment (SIGINT unit), East Germany (redefected)

Kaarlo Tuomi, 1959: GRU illegal sent to the United States; testified in 1963 against illegals who were tasked with providing information about rocket-launching sites, nuclear weapons shipments, and troop movements

Mikhail Strygin, 1959: Diplomatic cover in Burma (failed defection)

Yuriy Pyatakov, 1966: Worked aboard a Soviet SIGINT collection ship (redefected)

Anatoliy Chebotarev, 1971: Diplomatic cover in Belgium; reported on GRU SIGINT collection against NATO (redefected)

Nikolay Petrov, 1972: Diplomatic cover in Indonesia; ran an agent in the Indonesian Navy (redefected)

Yevgeniy Sorokin, 1972: Diplomatic cover in Laos (redefected)

Vladimir Rezun (pen name Viktor Suvorov), 1974: Diplomatic cover in Austria; published several books that describe GRU organization and methods

Viktor Korolyuk, 1980: Interpreter during East-West troop reduction negotiations in Vienna

Sergey Bokhan, 1985: Diplomatic cover in Athens; provided information about Greek sources who reported naval installations, the plans for the U.S. Stinger surface-to-air missile, and satellite antennae

Andrey Remenchuk, 1987: Diplomatic cover in Canada (redefected)

Yuriy Smurov, 1988: Secretariat of the International Civil Aviation Organization in Montreal

Aleksandr Krapiva, 1991: Soviet mission to the UN in Austria

Sergey Dvyrnik, 1991: GRU position and type of intelligence collected not publicly available

Stanislav Lunev, 1992: ITAR-TASS correspondent in the United States

Sources: Figure created by author from multiple sources, including Ismail Akhmedov, In and Out of Stalin's GRU: A Tatar's Escape from Red Army Intelligence *(Frederick, MD: University Publications of America, 1984); Viktor Suvorov,* Inside Soviet Military Intelligence *(New York: MacMillan, 1984); A. Korzun and V. Filin, "Stirlits Worked at the 'Aquarium': 13 Little Known Facts from the Life of the Main Intelligence Directorate," Komsomolskaya Pravda, October 10, 1992, 3, translated by the Foreign Broadcast Information Service, Central Asia, Military Affairs, JPRS-UMA-92-044, December 9, 1992, 1.*

In addition to defectors, Western intelligence services ran several prominent penetrations of the GRU during and after the Cold War that provided valuable information about the organization:

- Petr Popov (1953–58)
- Dmitriy Polyakov (1960–85)
- Oleg Penkovsky (1961–62)
- Sergey Skripal (1995–2001)

Petr Popov was familiar with Soviet illegals operating in the United States and other NATO countries. He provided information about the organization of the Soviet military, the structure of the GRU, and the names and operations of Soviet intelligence agents in Europe. The United States ran Dmitriy Polyakov for 25 years until he retired from the GRU as a general officer. He provided huge amounts of information about Soviet weapon systems and Soviet concerns about U.S. weapon systems. Oleg Penkovsky had access to Soviet missile information, and he provided indications that the Soviet Union could place missiles in Cuba. He also provided large amounts of information about Soviet military doctrine and strategy, which was at the foundation of intelligence collection. Although Penkovsky suggested that the United States plant small nuclear devices around Soviet military and government headquarters to decapitate the Soviet government, the United States never took the recommendation seriously. Sergey Skripal had access to the GRU personnel department and could identify hundreds of GRU officers operating under diplomatic cover abroad.[369]

These defections and penetrations combined provided a window into how the GRU operated and what its priorities were. Dozens of espionage investigations and arrests, some of which were the result of defections and penetrations, yielded further insights into what Soviet intelligence was trying to acquire and, in some cases, what it successfully acquired.

In the view of Russian military commentator Pavel Felgenhauer in 2005, the GRU not only collected and analyzed military intelligence, but it also used its access to senior Russian decisionmakers to influence their decisions and provide greater emphasis on Russian military resource needs:

> Through the GRU, the General Staff controls the supply of vital information to all other decisionmakers in all matters concerning defense procurement, threat assessment, and so on. High-ranking former GRU officers have told me that in Soviet times the General Staff used the GRU to grossly, deliberately, and constantly mislead the Kremlin about the magnitude and gravity of the military threat posed by the West in order to help inflate military expenditure. There are serious indications that at present the same foul practice is continuing.[370]

If Felgenhauer's assessment is correct, the GRU may intentionally exaggerate the capabilities and intentions of adversarial military forces, fueling an even greater aggressiveness to collect intelligence on that threat.

FOUNDATIONAL MILITARY INTELLIGENCE

Foundational military intelligence is the information needed for planning and conducting military operations and the basis on which a military makes decisions about what weapons to procure, what military doctrine to develop, and how to train its forces. The Soviet Union placed a high priority on collecting foundational military intelligence before the Cold War began and continued to do so throughout that period.

Even before World War II ended, the GRU tasked its *rezidentura* in Ottawa to collect foundational military intelligence on U.S. and Canadian forces. According to the materials that Igor Gouzenko brought with him when he defected, Moscow tasked GRU *rezidenturas* to recruit people in military services and collect military organizational data, including information about U.S. troop units in Europe and transfers of units to the Pacific Theater. The Ottawa *rezidentura* received a requirement to collect the locations, strengths, and future plans of specific U.S. divisions and corps, as well as the establishment of a U.S. Army headquarters in Germany, its location, and the identity of its new commanding officer. The GRU headquarters telegram that tasked this collection began with the caveat: "It is very important that we receive this information."[371] The GRU also tasked the Ottawa *rezidentura* to collect information about future weapon systems, inventories, production projections, guns, shells, small arms, optical and radio equipment, automobiles and tanks, chemical warfare equipment, and the details of plants producing them—all while the Soviet Union was still a supposed ally.[372]

Other defectors provided information about Soviet SIGINT collection against U.S. ports and weapons production. U.S. espionage cases displayed a consistent requirement for foundational military intelligence, including information about weapon systems, troop movements, ship capabilities, repair manuals, airstrip capacities, missile sites, naval installations, and

NATO war plans. The United States was not the only target. Defectors and espionage cases provided information about Soviet targeting of military information across Europe and Asia.

Today, Russia follows, or attempts to follow, a similar plan—conducting intelligence to understand foreign military forces to the level that, if Russia needed to face them in battle someday, it would know how to defeat them. From 2016 to 2021, arrests of military-related suspects committing espionage for Russia have occurred in Canada, Poland, Hungary, Greece, Slovakia, Estonia, Austria, the United States, and Italy. These espionage subjects have had access to their own government's classified information and NATO information.

Military Intelligence in Wartime—Test Cases

Georgia, Ukraine, and Syria are test cases for how Russian intelligence operates in a modern combat environment. Analysis of those conflicts helps to understand how Russia employs military intelligence before and during military operations. Although Russian military leaders talk about a blurred line that separates peacetime and wartime,[373] an analysis of the methods that Russia has applied on the battlefield in Georgia, Ukraine, and Syria, contrasted with the methods Russia has used elsewhere, makes it clear that Russia is willing to go further where there is an active military conflict than where there is not. Russia uses military warfare tactics in Ukraine, for example, but does not go to the same lengths of conducting active military operations in the United States or EU countries.

When Russia launched a short war against the much smaller Georgian military in 2008, its performance revealed gaps in Russian military planning and execution capabilities.[374] However, Russia also introduced an innovation during that conflict: conducting computer-based actions in concert with military actions. For example, Georgian government websites were disrupted simultaneously with Russian military actions inside Georgia.[375] Although entities that claimed no connection to the Russian government conducted the disruption operations, and the operations had little military significance, this marked the first instance of such a combination of physical and virtual attacks in a military conflict.[376] On October 28, 2019, GRU-sponsored hackers again attacked Georgian Internet providers and damaged websites, including those of the Georgian government, judicial officers, media, and businesses, indicating a continuing wartime footing in Russia's mind.[377] These attacks require intelligence before execution, which Russian military intelligence collectors probably obtained through a combination of Soviet-era knowledge about Georgian infrastructure facilities and more recent intelligence collection that identified specific sites and avenues of approach.

For Russia, Ukraine is an unreserved wartime target, where Russia has applied all intelligence disciplines, characteristic of how it might operate in other military environments. On the HUMINT front, Russian officers in Kiev had many Soviet-era personal ties with their Ukrainian counterparts, making it easy to find recruitments inside the Ukrainian military. Ukraine expelled a Russian military attaché in May 2014 for collecting information about Ukraine's cooperation with NATO.[378] As the counterintelligence environment in Ukraine became more hostile for Russian collection after Russia annexed Crimea in 2014, Russia moved to neighboring countries to conduct intelligence activities related to Ukraine. The Moldovan government expelled five reported GRU officers in 2017 for trying to recruit fighters for the Russian-backed insurgency in eastern Ukraine.[379]

Russian computer-based operations in Ukraine show a refinement of Russia's use of them in concert with military actions, which in each case has relied on previously collected intelligence. As in Georgia, but on a larger scale, Russia conducted computer-based attacks to disrupt the Internet in Ukraine while undeclared Russian forces were seizing control of Crimea in 2014.[380] Those attacks required detailed intelligence about the nature of the communication systems in Crimea and the rest of Ukraine, which, as in Georgia, was probably a mix of both historical knowledge and more recent collection. From 2014 to 2016, the GRU exploited an intrusion into an Android application used by Ukrainian artillery forces to process artillery targeting data, which required penetration of that Android application prior to its use in combat. Over 9,000 Ukrainian artillery personnel used the application, and the intrusion contributed to heavy artillery losses.[381] In October-November 2018, a Russian-origin phishing campaign targeted Ukrainian government computers in the weeks preceding the November 2018 seizure of Ukrainian fishing vessels in the Sea of Azov. The targets possessed maritime information directly relevant to the seizure,[382] and a Russian military operation followed soon after this intelligence collection.

Syria has been a testing ground for new Russian tactical military intelligence capabilities tied to operations. Russia has used space-based sensors in Syria and, for the first time, from 50 to 70 drones for intelligence, surveillance, and reconnaissance (ISR), as well as targeting. Targeting intelligence and video footage are reportedly provided simultaneously to the Russian command staff in Hmeymim, Syria, and to the General Staff in Moscow. Russia is perfecting what it calls the "reconnaissance-strike complex," which means using collection sensors for real-time targeting of precision-guided munitions. A similar concept is called "net-centric warfare" in the United States. Since 2015, Russia has rotated many of its military commanders through Syria on three-month deployments, using Syria as a school for training officers in modern warfare and these new ISR-driven tactics.[383] Russia has fielded several of its newest reconnaissance aircraft in Syria to test their capabilities and to refine the doctrine regarding their use (see Chapter 9). Russia has also developed intelligence-sharing relationships with the players in the Syria conflict. Since 2015, Iraq, Russia, Iran, and Syria have had a joint intelligence center in Baghdad where they share intelligence and coordinate military operations. Russia gains much from its tightly controlled intelligence-sharing relationships, which allow it to steer other countries selectively toward its priorities and recruit officers from its allies for influence and collection purposes.[384]

STRATEGIC FORCES AND STRATEGIC MISSILE DEFENSE

Nuclear weapons are at the top of Russia's military intelligence collection requirements and have been since the beginning of the Cold War. While the Soviet Union was involved in active military operations only a few times during the Cold War, it was involved in a nuclear standoff throughout the entire period. Even during World War II, Russian military and civilian intelligence services sought to understand the West's nuclear capabilities and intent, reflexively assuming that it was always directed at annihilating the Soviet Union.

Soviet intelligence services began to focus on atomic weapons development several years before such weapons were ever used. GRU defector Igor Gouzenko wrote that as early as 1942, "the word 'uranium' was listed among the more frequently used phrases in the secret cipher codebook of the director of Military Intelligence in Moscow."[385] Soviet intelligence used the code word "ENORMOUS" to describe its collection of information about atomic programs. This same codeword continued to be used into the 1950s; Yevgeniya Kartseva (aka Petrova), a KGB officer who defected in 1954, noted that she first encountered that code word in a message to Canberra 15 days after an atomic test, presumably referring to the British nuclear test conducted in the Australian desert in October 1953.[386] The first espionage cases after World War II, including Julius and Ethel Rosenberg and David Greenglass in the United States and Klaus Fuchs and Alan Nunn May in the United Kingdom, involved penetrations of the U.S. nuclear weapons program. Both military and civilian intelligence services sent illegals to the United States in the late 1940s either to become penetrations of the nuclear weapons program themselves or to handle penetration agents. Today, Russia probably uses all available collection methods, especially humans and signals, to satisfy its requirements for intelligence on this priority target. Computer intrusions probably are not as good a source of information about strategic weapons because of tight security.

During the Cold War, espionage cases showed a continuous effort by Soviet and Warsaw Pact intelligence services to target the U.S. Strategic Air Command, the B-2 bomber, strategic submarine forces, theater and intercontinental nuclear-armed missiles, and ballistic missile research (see Figure 19). The baseline Soviet assumption was that the United States had a nuclear capability that it intended to use offensively. Espionage cases of German civil servants also yielded significant information about U.S. and

NATO military capabilities; for example, Margaret Höke, a secretary in the German Chancellor's Office, provided U.S. plans to place Pershing II missiles in Germany.[387]

Figure 19. Strategic Forces-related U.S. Espionage Cases

William Henry Whalen, 1959–66: U.S. troop deployments and Strategic Air Command nuclear retaliatory strike plans

John William Butenko, 1963: Research on the Strategic Air Command

Gary Lee Ledbetter, 1967: Information about the Polaris submarine piping systems

Clyde Lee Conrad, 1974–88: NATO's plans for fighting a war against the Warsaw Pact, including detailed descriptions of nuclear weapons and plans for movement of troops, tanks, and aircraft; handled by Hungarian and Czechoslovakian services

James Durward Harper, Jr., **1975–83:** Minuteman ICBM and ballistic missile research; handled by a Polish service

Ruby Louise Schuler, 1979–83: Minuteman ICBM and ballistic missile research; handled by a Polish service

Christopher M. Cooke, 1980–81: Strategic missile capabilities

Thomas Patrick Cavanagh, 1984: Technical research on the B-2 bomber

Sources: Figure created by author from multiple sources, including Frank J. Rafalko (ed.), CI Reader: American Revolution Into the New Millennium *(Washington, DC: Office of the National Counterintelligence Executive, 2004); Katherine L. Herbig,* Changes in Espionage by Americans: 1947-2007 *(Monterey, CA: Defense Personnel Security Research Center, 2008).*

In the 1980s, the Soviet government initiated an intelligence collection emphasis called Operation RYaN, which was an acronym for the Russian phrase *ракетно-ядерное нападение* (nuclear missile attack). According to KGB defector Vasiliy Mitrokhin, RYaN was founded on the assumption that the Western alliance, especially the United States and Great Britain, was preparing for a nuclear attack on the Soviet Union. RYaN was a historically unusual instance in which Soviet civilian and military intelligence collaborated worldwide beginning in the early 1980s, although their collection yielded little, as no such Western preparations existed. This emphasis on nuclear missile attack led to the Soviet alarm during the 1983 NATO Exercise Able Archer, which the Soviet nuclear warning system interpreted as a possible nuclear attack. A memo from KGB First Chief Directorate Chief Vladimir Kryuchkov, which enumerated Russian intelligence priorities for the year 1984, included the instruction to collect intelligence on "preparation by the USA and its allies of a surprise nuclear attack on the Soviet Union; plans and actions by the main adversary to increase its strategic military potential and to step up the American military presence in Western Europe and other strategically important areas of the World."[388] According to the Soviet leadership, NATO's preparations included "the expansion of sabotage-training intelligence schools and increase in the recruitment of émigrés from the Socialist countries and persons who know the language of these countries, and the creation of émigré military formations and sabotage and intelligence teams."[389] For the Russian government, strategic missile defense has also been a dangerous development. If U.S. strategic missile defense worked as planned, it would nullify Russia's most capable military deterrent—its nuclear force. According to Mitrokhin, the Soviet leadership viewed Reagan's Strategic Defense Initiative, better known as Star Wars, as part of a program to prepare the American people psychologically for nuclear war.[390]

Although there are few publicly available cases directly related to Russian collection of strategic missile defense information, the historical record of Soviet collection on strategic military systems, coupled with current Russian rhetoric about the supposed threat posed by missile defense, indicates that missile defense is a major target of Russian concern. In one possible case, GRU computer-based collectors conducted a nearly two-year effort beginning in March 2015 to intrude into Danish Ministry of Defense computers. The operation began less than two weeks after Denmark announced plans to participate in NATO's missile defense system, and Western analysts have assessed that Denmark's decision prompted the collection operation.[391] The 2016 Foreign Policy Concept of the Russian Federation states, "Russia views the creation of the global missile defence system by the US as a threat to its national security and reserves the right to take adequate retaliatory measures."[392] The Russian government opposes what it calls "unilateral, unrestricted actions by States or groups of States to build-up missile defense systems that undermine strategic stability and international security."[393] As an analyst at Lawrence Livermore National Laboratories wrote in 2018:

> A major aspect of Russian anxieties about the Aegis Ashore [ballistic missile defense] deployments is a sincere, if paranoid, fear that the system will be used offensively in a first strike against Russia as part of a U.S. grand strategy of unilateralism and global dominance that entails encircling and constraining Russia. The transfer of U.S. nuclear weapons to the Aegis Ashore base in Romania would support this Russian narrative.[394]

Russian clandestine collection to fully understand and counter the missile defense threat, similar to RYaN of the 1980s, undoubtedly accompanies Russia's public declarations of concern and employs all collection disciplines.

WARTIME STRATEGIC TARGETS

Russia's military intelligence collection is an outgrowth of Russian military doctrine. An element of Russian military doctrine that envisions preparing for and winning the initial period of war is the concept of *Стратегическая Операция по Поражению Критически Важных Объектов* (Strategic Operation for the Destruction of Critically Important Targets, SODCIT). This concept governs a multidomain operation intended to destroy critical enemy facilities in the initial stage of war to dissuade the adversary from escalating into full-scale war.[395] SODCIT is divided into three categories of targets, based on the level of conflict that they affect:

- Tactical targeting directly focuses on enemy military forces to prevent them from posing a threat to Russia.

- Operational targets take one step back to disrupt the capabilities that directly support those military forces, including command and control and logistics.
- Strategic targets are foundational capabilities that allow a government to field and maintain a military force.

As is often the case in Russian military planning, the language defining military concepts is defensive, not offensive. Thus, the definition of a critically important target can be extracted from Russian government documents on civil defense: "a target (or facility), the destruction or suspension of functionality of which would lead to loss of control of the economy of the Russian Federation, of a subject of the Russian Federation, or of the territorial unity of the Russian Federation, her unrecoverable negative change (destruction) or a substantial lowering of the security of the vital functions of the population."[396] These same concepts apply in reverse in Russian offensive targeting. The objectives of destroying a critically important target are to prevent the adversary from being able to conduct war by:

- Disrupting national command and control.
- Destroying strategic strike capabilities.
- Destroying military forces and stockpiles.
- Disrupting governance at the national and regional level.
- Disrupting the means of production and transportation and impeding the embarkation of follow-on forces and critical supplies.

During the Soviet era, the Soviet government was convinced that a conflict would inevitably break out with the major capitalist powers. Soviet propaganda constantly trumpeted the threat of capitalist powers starting the next war. Vasiliy Mitrokhin's materials indicate that the KGB was collecting information about critical infrastructure sites across NATO countries at least as early as 1959, preparing for what now could be called SODCIT. This collection aimed at preparing target packages and infiltration plans for covert teams tasked with damaging and disrupting critical infrastructure sites during a future conflict, thereby reducing the target country's ability to support the conflict. Both the KGB Thirteenth Department and the GRU conducted similar collection, sometimes duplicating or conflicting with each other, as each planned for a future war with the West. Targets included electrical power transmission lines, oil pipelines, communication systems, and major industrial complexes in nearly all NATO countries.[397]

These strategic operations were a continuation of sabotage missions that Soviet state security organizations had been responsible for conducting since the beginning of the Soviet era. In the early Soviet days, sabotage was directed against the capitalist powers with the hope of catalyzing local revolutions to overturn the government and install a Bolshevik-style revolutionary government in its place. When Stalin changed the Soviet philosophy from world revolution to socialism in one country, he also shifted the focus of sabotage operations from prompting revolution in vulnerable countries to contingency planning in the major capitalist powers, such as the United Kingdom, France, and the United States.

After World War II, during which sabotage operations were directed primarily at German targets, the Soviet Union returned to preparations for these operations in the Cold War context. KGB and GRU intelligence collection operations focused on building target packages for critical infrastructure sites, including detailed information about terrain, landmarks, climate during different seasons, prevailing winds, populated areas, and local customs. Target packages would support the infiltration of *диверсионно-разведывательные группы* (diversionary-intelligence groups, DRGs), teams of operatives that would clandestinely infiltrate by air or sea to conduct the critical infrastructure sabotage operations.

After KGB officer Oleg Lyalin defected in the UK in September 1971, he shared intelligence on his work for the KGB Thirteenth Department (later renamed Department V), where he was responsible for identifying, collecting information about, and planning sabotage attacks against critical infrastructure sites. Lyalin reported that his targets included public utilities, railways, government and military communications, government offices and continuity-of-operations sites, and emergency food supplies. Based on the information he was tasked with collecting, Soviet air- and seaborne sabotage units would attack these targets if war broke out with the West. Lyalin was also supposed to develop a group of agents inside the United Kingdom that would support sabotage operatives when they landed. According to Lyalin, the KGB did not conduct what he called "industrial sabotage" in peacetime. The Soviet Union instead planned to begin sabotage operations during the period of crisis that preceded the outbreak of war; during that period, sabotage measures would include the demoralization of the civilian population and disruption of the country's political and economic life.[398] Lyalin also identified his counterpart responsible for performing the same mission in the United States, and he provided information about a plan to land sabotage agents on the California coast. As later KGB defector Oleg Kalugin wrote, every large KGB rezidentura around the world had one Department V officer tasked with preparing for future war.[399]

Mitrokhin similarly claimed that infrastructure targeting was not limited to the United States and Great Britain. He reported that planning for sabotage was more active in Iran than in any other non-Western country. In the 1960s and 1970s, Soviet intelligence services drew up detailed plans to attack royal palaces, major ministries, the main railway station, police and SAVAK secret police headquarters, TV and radio buildings, electricity transmission stations, and telephone exchanges. None of these targets had proceeded past the planning stages before Lyalin defected in 1971.[400]

Ukraine

Russian collection on critical infrastructure targets continues today, and the infrastructure attacks launched in Ukraine since the annexation of Crimea are the result of previous intelligence collection to prepare for sabotage operations. For Russia, Ukraine is an easier target than most countries, because it was formerly part of the Soviet Union, and thus Moscow is familiar with its infrastructure networks, which are largely remnants from the Soviet era. The combination of that baseline knowledge and Russia's ability to penetrate Ukrainian computer systems has made Ukraine an easy target for these types of operations.

Just as with foundational intelligence collection, the use of intelligence services for military targeting is more intense in Ukraine than in other parts of the world, which is evidence that Russia sees its relationship with Ukraine as an active military conflict. Targets in Ukraine have repeatedly included the strategic facilities identified in the SODCIT concept.

Ukraine has experienced repeated massive computer intrusions and attempted intrusions into its government and electric power infrastructures. For example, in 2015, the Security Service of Ukraine (SBU) reported a Russian spearphishing email attack on Ukrainian computer systems aimed at disrupting government and law enforcement networks, primarily those engaged in operations in Eastern Ukraine.[401] In December 2015, remote network intrusions caused unscheduled outages in three Ukrainian regional electric power distribution companies impacting approximately 225,000 customers, and malware was also found in Ukrainian companies in other critical infrastructure sectors. The attack was reportedly synchronized and coordinated, probably following extensive reconnaissance of the victim networks.[402] The GRU computer intrusion team known in the West as Voodoo Bear is believed to be behind the attacks.[403] This group has conducted sabotage operations throughout Ukrainian society, destroying hundreds of computers at media companies, deleting or permanently encrypting terabytes of data on government computers, and paralyzing infrastructure, including Ukraine's railway ticketing system. Voodoo Bear's known operations are consistent with an entity supporting Russian military and political objectives through targeted espionage and sabotage operations.[404] In December 2016, Russian-origin malware attacks again targeted Ukrainian electrical grids, during which a power distribution station near Kiev unexpectedly switched off, leaving the northern part of the capital without electricity. Ukrainian investigators assessed that the attacks might have been a proof of concept rather than a full attack.[405]

The most damaging Russian attack targeting Ukraine occurred in 2017, when the NotPetya virus was unleashed in Ukrainian computer networks.

On June 27, 2017, a series of cyberattacks targeted the websites of Ukrainian organizations, including banks, government ministries, newspapers, electricity firms, and state-owned enterprises such as Boryspil International Airport, Ukrtelecom, Ukrposhta (postal service), State Savings Bank of Ukraine, and Ukrainian Railways. The radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline during the attack. The malware overwrote and permanently damaged files in the infected computers, despite the malware's displayed message to the users indicating that all files could be recovered "safely and easily" by meeting the attackers' demands and making the requested payment in Bitcoin currency.[406]

The NotPetya attacks damaged more than just Ukrainian targets. Although the attacks were probably launched to cause SODCIT-like damage and degrade Ukraine's ability to conduct warfare against Russia, the GRU officers who released the virus either failed to calculate the vast collateral damage that NotPetya would cause or thought little of it. Most prominently, the virus also caused severe disruptions in the operations of the Danish Maersk shipping line, along with other probably inadvertent targets around the world. *Wired* magazine quoted former U.S. Homeland Security adviser Tom Bossert as saying, "While there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory. That's a degree of recklessness we can't tolerate on the world stage."[407]

Russia did not stop there. In July 2018, Ukraine's SBU claimed to have thwarted an attack on network equipment belonging to the LLC Aulska chlorine plant in eastern Ukraine. The attack was allegedly geared to disrupt the stable operation of the plant, which provides sodium hypochlorite for water treatment.[408] Such a disruption could have caused massive civilian damage.

The above examples are all manifestations of the "industrial sabotage" attacks for which Lyalin collected intelligence in the 1970s. In Ukraine, they have progressed beyond the collection phase to execution. Due to today's global computer-network accessibility and Russia's pre-war infrastructure collection, events in Ukraine probably demonstrate how Russia would operate in a military conflict elsewhere.

Outside Ukraine

Another infrastructure-level attack took place in 2018 that had nothing to do with Ukraine. In February 2018, a crippling computer virus labeled the "Olympic Destroyer" brought down the IT infrastructure for the Seoul Korea Olympics. Investigators were initially confused about attribution because the attack used elements that pointed to multiple countries' malware signatures; however, a computer forensic investigator found a conclusive signature that showed a Russian hand, with all the others being false flags. This attack turned out to be a GRU operation deliberately obscured behind other misleading pieces of evidence.[409]

Why would Russia launch such an attack that is not part of a military campaign? As discussed in Chapter 4, Russia launched computer intrusions into the World Anti-Doping Agency in 2016 to collect information about the investigation into a Russian state-sponsored program to provide performance-enhancing drugs to its athletes. That investigation concluded that Russia did, in fact, have a systematic doping program, resulting in the ban on Russian athletes' participation in the 2018 Olympics. The "Olympic Destroyer" probably is the next stage in what Russia sees as a political war being waged against its global reputation. Computer security experts predicted similar attacks on the 2020 Olympics in Japan; however, postponement of those Olympic Games, due to the global coronavirus pandemic, appears to have derailed any such plans.

STRATEGIC CONTINGENCY COLLECTION

Today, when the Russian media talks about diversionary intelligence groups (DRGs), they refer to repelling foreign DRGs invading Russian soil, not deploying DRGs to infiltrate foreign soil. In the post-Soviet era, however, Russian collection for future wartime sabotage operations continues, as indicated by the prevalence of computer-intrusion attempts and operations into critical infrastructure sites in the United States and other countries. The U.S. Department of Homeland Security and Department of Defense have issued multiple warnings about surveillance of critical infrastructure targets, probably as a modern equivalent to the longtime Soviet practice of preparing for future war.[410] Infrastructure penetrations for intelligence collection purposes and to prepare for future warfare have been reported in the United States as recently as October 2020.[411] Other countries—such as Germany, the United Kingdom, and Israel—have reported similar penetrations.[412] Targets include nuclear power, electric utilities, water, aviation, telecommunications, critical manufacturing sectors, and commercial facilities, similar to those that Oleg Lyalin discussed in 1971.

This computer-based collection coincides with other types of intelligence collection that appear to be coordinated. U.S. counterintelligence officials have observed Russian intelligence personnel traveling to remote places across the United States, standing outside a particular site for a few minutes, sometimes holding a device in their hands, and then getting back into their cars and driving off. The U.S. counterintelligence community has correlated this activity with the locations of communications nodes associated with U.S. military bases. The U.S. Government has also noted that Russian Open Skies Treaty flights sometimes overfly U.S. critical infrastructure sites at the very time that Russian officers on the ground travel to those sites. The two types of collection appear to be coordinated to map critical U.S. military communications infrastructure elements that could be targeted for sabotage if war broke out with the United States.[413] Russian collection against communication nodes is taking place in U.S-allied countries as well. In early 2020, Irish police arrested Russian intelligence personnel who were apparently mapping the precise locations of landing points for undersea fiber-optic cables in Ireland.[414]

Russia's strategic contingency collection assets may also include a Russian undersea research ship and submarines, which reportedly troll around the ocean, possibly surveilling undersea communication cables—a critical element of the world's telecommunications infrastructure. According to a 2015 *New York Times* article, the United States that year closely monitored the Russian oceanic research ship *Yantar*, which is equipped with two self-propelled deep-sea submersible craft, as it cruised off the U.S. East Coast toward Cuba, where one cable lands near the U.S. naval base at

Guantanamo Bay. Naval officials claim the ship and the submersible craft are capable of cutting cables miles deep beneath the sea.[415]

Some analysts, including a self-described Canadian military buff, have questioned the legitimacy of the U.S. assertion that the *Yantar* is surveilling undersea cables, claiming instead that the *Yantar* is exploring the locations of sunken Russian and other countries' ships and submarines, and that minor damage frequently occurs to undersea telecommunications without major disruptions.[416] Nevertheless, in 2017, British defense officials warned that the Russian Navy poses a potentially "catastrophic" threat to undersea cables.[417] NATO also has assessed that Russia is capable of attacking undersea cables and causing massive disruptions to commercial and government communications.[418] In February 2020, the U.S. Department of Defense published its 2021 budget request, in which it included a map overlaying Russian and Chinese naval activity over international undersea communications cables. Although the purpose of the map was to advocate for greater funding for the U.S. Navy, it makes clear that foreign naval forces are potentially threatening the global economy by putting undersea cables at risk.[419]

CONCLUSION: PREPARING FOR WAR

Up to now, none of these collection cases, whether by computer, Open Skies aircraft, on-the-ground officer, or seaborne system, has resulted in sabotage to critical U.S. or NATO infrastructures. However, Russian military intelligence activities in Ukraine and Syria show how Russia operates in a wartime environment. When Russian troops occupied strategic positions in Crimea in 2014, special operations forces detachments took over the Simferopol Internet exchange point and selectively disrupted cable connections elsewhere on the Ukrainian mainland. That operation left Crimea isolated from the global information environment, allowing Russia to dictate the information flow into and out of Crimea.[420] Russia probably is collecting intelligence now to prepare for similar operations in case of war with the West.

All three military collection directions—foundational, strategic weapons, and contingency military collection—are priorities for Russian intelligence services today. Russian services, especially the GRU, use all collection disciplines to target those topics. As Russian military leaders continue to assume that the West in general, and the United States in particular, are planning a surprise attack on Russia, they will use all available tools to prepare for that attack.

CHAPTER 7

COVERT ACTIVITIES

Russian intelligence services mix the concepts of intelligence collection and covert activities closely together. While intelligence collection supports decisionmakers with information, covert action executes the decisionmakers' plans and policies. They are both elements of the Russian concepts *разведка* or *razvedka*, which translate into English as "intelligence" or "reconnaissance." The preceding chapters have covered types of intelligence collection. This chapter will cover the other side of *razvedka*: covert activities, including the three major categories of political operations, undeclared military operations, and assassination operations.

In wartime, military members covertly penetrate the enemy's territory to conduct diversionary actions. Russia commemorates many covert operators from World War II as heroes who saved Russia from the Nazis. The Soviet Union organized thousands of partisans behind German lines who extended the reach of Soviet intelligence services and helped to adapt Soviet operations to local conditions. In some cases, those partisans became the post-war leaders of Eastern European countries, such as Josip Broz Tito in Yugoslavia and Władysław Gomułka in Poland. In other cases, Soviet partisan leaders were recognized as heroes, such as Anna Morozova and Imant Sudmalis, who were named as Heroes of the Soviet Union in the 1960s, and Aleksey Botyan, who was awarded the title Hero of the Russian Federation in 2007.

Soviet-era intelligence officer defectors give us insights into the lengths Russian military forces will go to execute covert military activities. Chapter 6 introduced the concept of *диверсионно-разведывательные группы* (diversionary intelligence groups, DRGs), based partially on information provided by KGB officers Oleg Lyalin, Oleg Kalugin, and Vasiliy Mitrokhin. During military warfare, these groups take intelligence collected about adversary targets and execute operations against them, with the goal of:

- Creating disorder in the rear area functions of the enemy.
- Disabling the enemy's transportation and communications.
- Spreading panic among the enemy's troops and civilian population.
- Collecting intelligence about the movements, dispositions, armaments, and numbers of the enemy's forces, its military-economic potential, militarily significant industrial facilities, and transportation and communications systems.
- Destroying the enemy's upper and middle command staffs and designated political and administrative personnel.

These actions are tools of military war. We see Russia using these operations in places where it considers itself to be involved in a military war, such as in Chechnya, Georgia, Ukraine, and Syria, and more recently in Libya. As noted in Chapter 6, Russia's use of the NotPetya virus against Ukraine reflects Soviet-era plans for operations to demoralize an adversary's population, disrupt its political and economic life, and diminish its ability to sustain war. As such, this activity is part of a military campaign, not a political campaign. However, for Russia, there is a difference between political warfare, which could occur in what most countries call peacetime, and military warfare, which occurs in a generally recognized wartime environment. Political warfare does not employ all the weapons of military war, but it is also not identical with peacetime.

While the West views the relationship with Russia as a tense peacetime one, Russia sees it as being in a political wartime environment. Russian analysts claim that the United States is already conducting a political war against Russia. They perceive a nefarious Western hand behind any event that has an anti-Russian tone, even where no such hand is involved. Russia views the "color revolutions" that occurred initially in former Soviet republics (Kyrgyzstan, Georgia, and Ukraine) and later in other countries (Syria and Libya) to be Western manifestations of covert political operations. Russian leaders similarly characterize the anti-Putin demonstrations that occurred in 2011-12 as Western political warfare. Russia believes that it must defend itself from Western disinformation and "Russophobia" (such as public claims of Russian spying around the world), Western undeclared military activities (such as Russia-alleged Western support to terrorists in Chechnya, Syria, and Libya), and Western assassination operations (such as the killing of Moammar Qadhafi).

Clandestine vs. Covert

The words clandestine and covert do not mean the same thing, even though they are often used interchangeably. Clandestinity conceals the operation, while covertness conceals the operator. Most of what has been discussed previously in this book falls into the category of clandestine activities—internal security and intelligence collection operations performed in such a way that they are not publicly visible. Clandestine means secret; something is done so that only those involved in it know it is happening. Most intelligence operations are clandestine, because if they became public, sensitive sources and methods could be damaged or eliminated. However, the sponsoring government does not usually hide its involvement in the operation. For example, when an intelligence service pitches a HUMINT source, the source usually knows for what government he/she is working, unless the service is using a false flag to deliberately misrepresent its affiliation.

Covert means the sponsoring government does not reveal its involvement. Although covert operations are usually clandestine in the planning stages, the result of a covert activity often becomes public, even intentionally. That includes covert sabotage, in which an object is damaged: for example, when a bomb explodes or a computer system goes offline. The primary element of covert activities is the phrase "plausible deniability," which means the action is visible, but the perpetrator's identity is hidden. This chapter discusses covert activities in which Russia tries to deny its involvement, albeit often unsuccessfully and with little plausibility.

Thus, Russia responds to what it views as an ongoing covert war with covert actions, such as political manipulation operations, which it sees as appropriate in a political war. However, during non-military war, these actions require more deniability since, if a country is found to have conducted them, they can escalate into a military war, which Russia is not eager to have happen.

COVERT OPERATIONS: POLITICAL WARFARE

During the Soviet era, the KGB conducted covert political operations labeled "active measures," a Cold War concept of covert political manipulation. Vasiliy Mitrokhin provided the following definition of active measures:

> Agent-operational measures directed at exerting influence on the foreign policy and the internal political situation of target countries in the interests of the Soviet Union and of other countries of the socialist community, the World Communist and National Liberation Movement, weakening the political, military, economic, and ideological positions of capitalism, undermining its aggressive plans, in order to create conditions favorable to the successful implementation of the Soviet Union's foreign policy, and ensuring peace and social progress.[421]

The Russian phrase *агентурно-оперативные мероприятия* (agent-operational measures) means clandestine intelligence methods. That is what placed active measures into the KGB's mission; however, the actions were covert because the Soviet Union sought to hide its sponsorship of the political manipulation operations that it conducted worldwide. The end goal of active measures was to create conditions favorable for implementing Soviet foreign policy. Mitrokhin's definition originated in the Cold War, so it includes the Cold War ideological narrative of the socialist vs. capitalist world. Today, that ideological element is gone, and Russian intelligence services no longer use the phrase active measures. Instead, as noted in Chapters 2 and 5, the SVR has a directorate labeled MS (*мероприятия содействия* or measures of support), which conducts equivalent operations today in a different ideological environment.

In a speech given in 1992, SVR Director Yevgeniy Primakov echoed much of Mitrokhin's definition, saying that "measures of support are those measures that are implemented so that the policies of Russia and our state proceed better and more efficiently." He continued:

> Let me give you an example. If it became known that a country is toughening its position and wants to prevent the G7 from providing large-scale economic support for the reforms being carried out in Russia, then intelligence methods can and should obviously be used to bring to public opinion and to the leaders of the G7 countries the desire of one of the member-states to shift the economic burden onto the shoulders of others and take advantage of the situation in order to generate support for their position on a territorial issue.[422]

Measures of support are sometimes equated with disinformation and propaganda, although they are more likely to be related to disinformation operations than propaganda activities. Propaganda is an overt act. It involves deliberately taking one side of an issue and making it look better, while sometimes denigrating the opposing side. Spreading propaganda is a normal practice in public diplomacy, political dialogue, and advertising, to which we are subjected every day. This undisguised act does not require clandestine activity, although intelligence activities can support propaganda by feeding it clandestinely acquired information that supports an overt theme.

Disinformation is the deliberate manipulation of information. It is a covert action and thus is more closely connected to intelligence and security services. According to Czechoslovakian intelligence officer defector Ladislav Bittman, the Cold War saw more than 10,000 Soviet and Eastern Bloc disinformation operations.[423] Political scientist Thomas Rid, who reported Bittman's statement, went on to say:

> Understanding 'cyber operations' in the 21st century is impossible without first understanding intelligence operations in the 20th century. Attributing and countering disinformation operations today is therefore also impossible without first understanding how the US and its European allies attributed and countered thousands of active measures throughout the Cold War.[424]

The pace of Soviet/Russian active measures operations has fluctuated, aligning with shifts in Russian foreign policy. During the 1950s and 1960s, active measures to counter U.S. military alliances and plans were relentless. These operations subsided in the early 1970s during the détente period, followed by an even greater intensity in the mid-1980s, and then a long ebb throughout the 1990s. In the late 2000s, disinformation operations began to rise again.

During the Cold War, the U.S. Department of State hosted an Active Measures Working Group that identified and attempted to counter Soviet disinformation operations. The group publicly declared in 1981 that "Moscow makes extensive use of 'active measures' to achieve its foreign policy objectives and to frustrate those of other countries."[425] This quote could apply today just as it did during the Cold War, although Russia no longer uses the phrase active measures to describe those activities. Over the last decade of the Soviet Union, Soviet intelligence actively cultivated numerous stories around the world to, as the State Department wrote in 1981, "achieve its foreign policy objectives, frustrate other countries objectives, and to undermine leadership in other countries."[426] (see Figure 20).

In some cases, the stories were completely manufactured with no truth to them at all, such as forged documents intended to derail the Middle East peace process in 1976;[427] the famous Operation INFEKTION, which claimed that the AIDS virus was manufactured in a U.S. military laboratory;[428] and the ghastly rumor that the United States harvested body parts from children in Latin America for transplants in the United States.[429] The Soviet Union manufactured and disseminated these absurd stories to a Third World audience that was inclined to believe any anti-U.S. information. In other cases, active measures narratives either twisted a real story in a Soviet direction or accentuated one side of a story and denigrated the opposing side to present a Soviet perspective.

Figure 20. Soviet-era Active Measures Campaigns

1977: Forged U.S. Department of State documents criticizing the Egyptian leadership

1977: Booklet "America's 200 Years"

1977–78: Campaign against enhanced radiation weapons

1979–80: Anti-Theater Nuclear Forces campaign

1983–87: Operation INFEKTION—AIDS virus disinformation

1984: "Reagan means War!"

1985: U.S. backing for the South African apartheid regime

1985: Counternarrative regarding U.S. grain shipments to the Soviet Union

1985: American militarization of space

1987: "Baby parts" stories—kidnapping to harvest organs disinformation

Sources: Figure created by author from multiple sources, including U.S. Department of State, Soviet "Active Measures": Forgery, Disinformation, Political Operations*, Special Report No. 88, October 1981; Thomas Boghardt, "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign,"* Studies in Intelligence *53, no. 4 (December 2009): 1-24; Calder Walton, "Spies, Election Meddling, and Disinformation: Past and Present,"* The Brown Journal of World Affairs *26, no. 1 (Fall/Winter 2019): 107-124,* http://bjwa.brown.edu/26-1/spies-election-meddling-and-disinformation-past-and-present/*; Seth G. Jones, "Russian Meddling in the United States: The Historical Context of the Mueller Report," Center for Strategic and International Studies Briefs, March 2019,* https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report.

Modern Russian disinformation campaigns focus on a consistent set of themes. The Russian government repeats these themes throughout Russia's information operations, whether they be overt, covert, or a crossover between the two:

- **Russia played the leading role in World War II.** Russia emphasizes its own role in World War II and vehemently criticizes any country that questions that narrative. The downplaying or countering of Russia's narrative in Estonia, Poland, and Czechia has met Russian overt and covert responses. Russia's advancing of its World War II theme slowed during the COVID-19 lockdown in Moscow in 2020, which prevented the Moscow celebration of the 75th anniversary of the defeat of Germany. However, the event went on anyway in a smaller and delayed form.
- **Russia is the victim.** Allegations made against Russia in international forums, such as when a Russian is arrested or expelled for intelligence activities, are often met with counter-allegations claiming that Russia is under threat of Western political attacks.
- **The United States is a source of instability.** Russian disinformation focuses on U.S. actions, often tying world events to the CIA. Russian disinformation during the MH17 shootdown investigation in 2014–15 attempted to recast the event into a CIA-sponsored plot to provoke a confrontation with Russia.[430]
- **NATO is a threat to international security.** Russian operations frequently criticize plans for NATO enlargement and exercises, while downplaying its own activities to increase its influence over other countries and hold massive military exercises.
- **The European Union is on the verge of collapse.** The COVID-19 pandemic allowed Russia to spread disarray in Europe through disinformation and by providing targeted support to some European countries while criticizing others.[431]

In Thomas Rid's 2020 book *Active Measures*, which recounts the history of disinformation campaigns from both the Soviet and Western directions, he translates the Soviet-era methods into a post-Soviet context, illustrating the continuity of Russian intent over 100 years. According to John Emerson, these operations, both historical and current, show a pattern of activity that can be described with four "Ds":[432]

- **Distort.** Twist real information; take a truth and recast it in a different light to make it either seem more or less attractive. Russia regularly does this with its narrative of World War II, an undeniably legitimate topic of discussion that Russia twists for its political purposes.[433]
- **Distract.** Draw attention away from real information, as with the 2014 shootdown of Malaysia Airlines Flight MH17 over Ukraine. Russian media created multiple conflicting stories, each of which had no validity, but all of which pointed responsibility away from Russia.[434] This was also the case with Russian operations to leak information about athletes from multiple countries supposedly violating doping rules to take the attention away from the Russian government's doping program.[435]
- **Dismiss, Deny.** Vladimir Putin himself boldly denied that Russian troops were involved in seizing Crimea or supporting insurgents in Ukraine,[436] or that the Russian government carries any responsibility for the attempt to assassinate former GRU officer Sergey Skripal in 2018.[437]
- **Dismay.** Inflame fear, hate, or disgust, such as the Russian-originated claims that German troops had raped a young girl in Lithuania in 2016.[438]

Russia uses a variety of channels to disseminate patently false or deceptively half-true information. These operations vary in their level of covertness and by how much clandestinely collected information supports them. Russian media channels are often used to distribute Russian disinformation, and Russian intelligence services occasionally feed clandestinely collected information into overt broadcasts. These campaigns do not acknowledge the Russian collection of the information, but they make no attempt to hide the Russian hand in disseminating it. Russia also uses illicit Internet channels to dump politically damaging or salacious material into the public domain, from which it can then draw this "information" into overt media "reports." These illicit channels include already existing leaker web sites (e.g., Wikileaks) or clandestinely created leaker websites (e.g., DCLeaks), which hide the Russian hand behind both the collection and dissemination of the information.[439]

Russian disinformation operations also employ overt non-Russian media channels, such as newspapers, social media platforms, and journalist forums, to insert politically damaging or divisive information and cause dissension and confusion. For example, a Russian-linked illicit Twitter site called "Anonymous Bulgaria" has become a platform for disseminating Russian disinformation, including claims that the United States sent weapons to the Islamic State in Syria.[440] Like Russia's illicitly created channels, Russian intelligence services use these non-Russian channels without revealing the Russian collection of information or the Russian hand behind its dissemination.

An item of disinformation may start in one channel and then be reinforced in the others, particularly from illicit or non-Russian channels into Russian media. For example, information about U.S. political campaigns that was leaked through illicit channels during the 2016 Presidential election period was later reinforced through Russian media channels and fed to non-Russian media. This practice follows a historical method used during the Soviet era, when the famous Operation INFEKTION of the 1980s initially planted an AIDS virus origin story in a non-Russian media channel and later broadcast it via Russian news media. One of Aleksandr Kaznacheyev's responsibilities when he served as a KGB co-optee in Burma in the late 1950s was to translate materials provided by Moscow into English for clandestine distribution as if they came from local sources. Local translators would then render the letters into Burmese and send them anonymously to local, often pro-Communist newspapers, reportedly from unnamed press correspondents. After the "Burmese articles" appeared in print, Kaznacheyev would translate them back into Russian and send them to Moscow, from where they would be disseminated globally via Soviet press as purportedly of Burmese origin.[441] Similarly, MH17 disinformation in 2014 used obscure web-based media services to post false material on the airliner shootdown initially, and then broadcast it via

Russian media when the perceived need arose to disrupt the investigation into the incident.[442]

Collection vs. Operationalizing

Key "who" and "how" differences exist between collecting intelligence and operationalizing it. Collection and disinformation operations are conducted separately but sometimes cooperatively. Correspondingly, per the 2018 U.S. Department of Justice indictment of GRU officers responsible for the hack and leak operations leading up to the 2016 U.S. elections, the hack portion of the operation was conducted by a different element than the leak portion.[443] Information used in leak operations may be collected through normal political collection using SIGINT, HUMINT, or computer-based methods (see Chapter 4), or it can simply be manufactured outright. The information is then handed to a covert action unit that operationalizes it. The same intelligence could also be used for other purposes, such as national security decisionmaking.

The GRU element called Unit 26165 is a SIGINT unit that collects information for various customers, including other GRU units responsible for covert operations. The unit, which is also known as the "GRU 85 Special Service Main Center," is located at 20 Komsomolskiy Prospekt, Moscow. Unit 26165 conducted the operation to penetrate emails associated with Hillary Clinton's presidential election campaign and the Democratic National Committee in 2016. The GRU officers arrested in the Netherlands while conducting a close access SIGINT operation against the OPCW in 2018 were also from Unit 26165. The same unit was involved in computer intrusion operations of the Dutch Safety Board in 2015, related to the publication of the MH17 crash report, and the World Anti-Doping Agency intrusions in 2018.

The leak, or covert action, portion of the 2016 U.S. election-related operation was conducted by an element labeled Unit 74455, also known as the "Main Center for Special Technologies" (GTsST). Located in the Moscow suburbs, Unit 74455 is an execution arm of the GRU—the covert action side of *razvedka*—responsible for sabotage and disinformation actions. This element is the computer-network equivalent of a DRG, conducting sabotage and covert operations behind adversary lines. In addition to the 2016 leak operations in the United States, Unit 74455 has been connected to multiple destructive computer-based attacks, including those that affected critical infrastructure elements in Ukraine and the "Olympic Destroyer" attack that targeted the Seoul, South Korea Olympics in 2018.[444] Members of Unit 74455 mostly conduct operations remotely.

Another GRU element, Unit 54777, also called the 72nd Special Service Center, is reportedly a psychological and disinformation operations unit that maintains front organizations, including InfoRos and the Institute of the Russian Diaspora; InfoRos was named in April 2021 U.S. sanctions as an organization that spreads false conspiracy narratives and disinformation promoted by GRU officials.[445] Unit 54777 spread covert Russian-sponsored messages during the annexation of Crimea. During the November 2018 Kerch Strait incident, the unit sent bogus text messages to Ukrainian soldiers in the border region calling on them to report for military service. Letters sent to members of the U.S. Congress in 2015 from a group calling itself "The Patriot of Ukraine" are also believed to have come from GRU Unit 54777; the letters claimed that the Ukrainian military is corrupt and sells weapons to the so-called "Donetsk People's Republic," and they demanded that U.S. decisionmakers take control of the Ukrainian military.[446] These covert influence operations are probably founded on intelligence collected from a variety of sources, twisted to a Russian narrative.

Members of yet another GRU element, Unit 29155, are accused of conducting covert operations across Europe, including assassination operations, such as against Sergey Skripal in 2018; political meddling in Ukraine, Moldova, Montenegro, Spain, and the United Kingdom; and sabotage operations in Czechia and Bulgaria. Unlike Unit 74455, this unit dispatches officers abroad to conduct physical actions, not remote computer-based actions. Press investigations have identified a Switzerland-based forward headquarters, led by a GRU officer previously accredited to the

World Trade Organization in Geneva, Switzerland, as a coordinating element for the unit.[447]

Western investigative journalist organizations have revealed these unit designations publicly, and consequently the GRU may have changed them. Nevertheless, the separation of responsibilities within the GRU for intelligence collection and covert action missions remains.

COVERT ACTIONS: UNDECLARED MILITARY ACTIVITIES

The second major field of Russian covert action is undeclared military activities. The military forces dispatched from Russia for these undeclared operations are sometimes directly affiliated with Russian government organizations and sometimes not, offering some level of deniability that persists at least long enough to accomplish the mission. The purpose of these forces is to fulfill Russian policy goals while trying to avoid the political cost or escalatory effect of conducting aggressive, often internationally objectionable, military operations.

Undeclared military forces usually employ either GRU Spetsnaz covert action personnel deploying undercover or former GRU Spetsnaz personnel operating as private forces. The GRU Spetsnaz is Russia's covert action arm, and it has a long history of fulfilling Russian political objectives. GRU officer defector Vladimir Rezun (pen name Viktor Suvorov) served as a Spetsnaz officer before becoming a GRU case officer, and he has written extensively about his training to conduct rear-area sabotage operations and covert infiltrations.[448] During the Cold War, the Spetsnaz competed with the KGB for supremacy in planning and conducting covert infrastructure attacks, like the operations Lyalin discussed in his debriefings (see Chapter 6). During the Cold War, Spetsnaz personnel operated covertly in Angola, Lebanon, Vietnam, and Cambodia and conducted sabotage and assassination operations in Afghanistan. They operated similarly during the Chechen wars and in the 2008 Russia-Georgia war. GRU Spetsnaz fosters a reputation as a war-hardened unit that can be called upon to go places where others cannot go.

Little Green Men in Crimea

In March 2014, Russian soldiers wearing unmarked uniforms began occupying government and military buildings in Crimea, paving the way for Russia's illegal annexation of the territory. This sequence of events resembled the August 1968 takeover by Spetsnaz forces of the main administrative buildings in Prague, Czechoslovakia, to pave the way for a Soviet-led invasion to quell the Prague Spring.[449] Although the Russian origin of the so-called "little green men" in Crimea, Ukraine, was subsequently indisputably established, the covert nature of the operation created deniability when the events were occurring in 2014. The resulting doubt allowed Russia to complete the operation. In April 2014, during the Crimea operation, BBC reported that the soldiers occupying Ukrainian government and military buildings were claiming to be Ukrainians or Cossacks, although even at the time, they were not pushing that cover very hard.[450] Russia, including Putin himself, referred to them as "self-defense forces" at the time. A year later, Putin acknowledged that the forces were Russian, but by that time, deniability was no longer necessary—Crimea was firmly in Russian control.[451]

Nongovernment Forces

In addition to Russian government forces operating without acknowledgment, Russia has also increasingly used nongovernment military forces managed by Russian corporations for covert military activities. According to an article in the *Atlantic* magazine, using nongovernment forces "allows Russia to enter a foreign, largely hostile environment with minimal risk, and to exploit both political and economic opportunities there."[452] Since 2014, Russian private military corporation soldiers have operated in Ukraine, Syria, Central African Republic, Sudan, Mozambique, and Libya. The deniability that these nongovernment forces create has allowed Russia to play two sides of those conflicts simultaneously, providing covert military support to its preferred side in the conflict, while claiming openly to be an honest broker. The forces' private status has also allowed Russia to disclaim responsibility for casualties and violence. In 2017, the Islamic State captured two fighters from the Russian Wagner Group in eastern Syria and paraded them before cameras. Had they been acknowledged as Russian servicemen, the outcry at home would probably have been vigorous. Instead, the Kremlin brushed aside their captivity, claiming they were "probably volunteers."[453]

Covert military forces are fulfilling Russia's foreign policy requirements, just as political warfare operations are, although at times their success is questionable. In 2018, Wagner Group forces famously attacked a position in Syria occupied by U.S. forces and were decimated.[454] In Mozambique, when Wagner Group forces arrived to support Mozambiquan forces fighting Islamist insurgents, the Russians were quickly overwhelmed and forced to retreat to a base; the Wagner Group forces were accused of being ill-prepared for jungle fighting and disrespectful of the Mozambiquan forces they were supposed to be supporting. Similarly, Wagner Group forces in the Central African Republic are reportedly facing similar difficulties working with locals.[455] On the other hand, the Wagner Group has seen success in Libya, where the group has been a major source of support to the forces of Gen. Khalifa Haftar, the rebel leader who controls the oil-rich eastern portion of Libya. The Wagner Group has deployed a larger contingent of forces to Libya than to other countries in Africa.

COVERT ACTIONS: ASSASSINATIONS

The third category of Russian covert activities is assassinations. Russian assassination operations have become a major topic of political and journalistic discussion in the West, with assassinations being reported both inside and outside Russia during the Putin era. The attempt on Russian oppositionist Aleksey Navalny's life in August 2020 thrust the issue into the spotlight again. While assassination operations are often merged in Western analysis, the Russian government does not define them all in one category.

Russia divides assassination operations into three groups of targets: military, political, and traitors. It also divides the venues for assassination operations into two general locations: inside Russia and everywhere else. Russia's approach to eliminating opponents in the three categories differs significantly inside Russia from outside Russia (see Figure 21). Inside Russia, military targets are by far the largest category, with assassination operations in the North Caucasus region of Russia far outweighing every other group. Military targets are also the largest category outside Russia, although the overall numbers are smaller than inside Russia. Political targets come next, although most of them also occur inside Russia; very few political assassination operations occur elsewhere. The third category, traitors, is exclusively external because Russia has other state security tools to deal with traitors inside Russia.

Figure 21. Russian Assassination Types

	Internal	External
Political	Oppositionists, critical journalists	Small number of anti-Putin political activists
Military	During counterterrorist operations	Syrian opposition, Ukrainian, and Chechen military leaders
Traitors	Dealt with through state security mechanisms	Small number of special cases

The Russian calculus for assassinating someone inside Russia is much different than doing so outside Russia. Although the instrumentality of assassination, such as the use of a bullet to the head or a certain type of poison, might cross the boundaries of internal and external operations, the sensitivity of operations outside the country is much greater than it is inside. This difference became clear following the assassination of Zelimkhan Khangoshvili, a Chechen militant leader, in Germany in August 2019,[456] which led to a German legal investigation and expulsion of Russian diplomats. That external-internal dynamic makes it especially surprising that the Russian government allowed Aleksey Navalny to be taken abroad for medical treatment after he was poisoned in Russia in 2020.[457] Navalny is an internal threat; when he returned to Russia in January 2021, the Russian government arrested him immediately upon arrival in Moscow and soon sentenced him to three and a half years in prison. Allowing Navalny to have treatment abroad that confirmed his poisoning may turn out to have been an error in Russia's assassination calculus.

Internal Assassinations

Russia views assassination operations inside Russia as a state security necessity, not an extreme act. Using violence to resolve internal political opposition is a natural trait of an authoritarian regime. The primary objective of an authoritarian regime is to retain control of the political environment by whatever means necessary, including by physically eliminating threats.

Internal Political. During the Soviet era, assassinations for political crimes were uncommon inside the Soviet Union; they were not seen as necessary because other methods were available to neutralize those who crossed a political line. In the early Soviet era, OGPU "troikas" (three-person extrajudicial teams of state security personnel) had the authority to order executions, and later simply making someone disappear was enough. Neutralizing internal opposition could be done using various methods, including sentencing dissidents to inhuman conditions in corrective labor camps or psychiatric hospitals. Although not overtly assassination, it often amounted to a death sentence.

More recently, the deaths of leading opposition figures, anticorruption activists, and critical journalists have become a common occurrence inside Russia, although the Russian government targets only leading oppositionists and the most vocal journalists for assassination. These include people like liberal politician Boris Nemtsov, journalist Anna Politkovskaya, and most recently opposition leader Aleksey Navalny. Although numerous journalists have been killed in Russia, their deaths have often come not at the hand of the central government, but probably instead by the order of individual powerful elites or criminal leaders—for example, when a journalist was getting too close to the truth regarding a criminal or corrupt enterprise. Journalists killed covering events in Chechnya are in yet another category, viewed inside Russia not as political targets but as the victims of war.

The threshold of activities that warrant a state security response is not absolutely clear, but there are activities that fall below those that would trigger an assassination operation (see Figure 22). Assassination is a relatively rare tool reserved for the most prominent oppositionists and critical journalists, those who become too popular for the ruling regime to tolerate. Navalny is the most recent, and his actions clearly crossed red lines in the Kremlin's analysis.

Figure 22. Russian Calculus for Action Against Internal Oppositionists

	Level of Oppositionist Activity	**Russian Government Response**
5	Become a symbol of the opposition and draw a major following	Arrest and sentence to extended prison time, but consider assassination
4	Lead an opposition group; gain prominence as an oppositionist figure or critical journalist	Arrest and sentence to extended prison time
3	Join an oppositionist group or actively participate in oppositionist activities; write critical material about the Putin regime	Arrest and hold for a short time in custody
2	Participate in oppositionist discussions online or in person	Initiate monitoring
1	Read oppositionist material	No immediate reaction

Source: Figure derived from work completed by National Intelligence University student, MAJ Teresa Haltom, in pursuit of the Master of Science of Strategic Intelligence degree in 2019.

Short of assassinations, internal political oppositionists are handled in various ways based on the degree of their perceived malfeasance. Some passive oppositionist actions do not even meet the threshold for an overt state security response but could attract increased monitoring of communication channels. People in this category are probably among the thousands whose personal information Russian government entities request from Russian Internet service providers (see Chapter 3). This level of opposition activity could also predicate a counterintelligence operation to recruit an individual as a double agent or an *agent provocateur*. A person must cross a threshold to be considered for arrest, including participating in oppositionist activities, like mass demonstrations, although these are not invariably the cause for arrests, as seen in Khabarovsk in 2020 when a crackdown did not immediately follow anti-Kremlin protests against the arrest of a popular regional governor. In contrast, mass demonstrations that followed the January 2021 arrest of Navalny crossed the threshold and led to thousands of arrests. Assassinations are considered only in the most extreme cases.

Internal Military. For Russia, leaders of anti-Russian militant or terrorist organizations are justifiable assassination targets wherever they are. They are not treated the same as, and are much more frequently attacked than, political targets. Internal military assassination operations are divided into those that occur in the North Caucasus specifically and those that occur elsewhere in Russia. In the North Caucasus, Russian state security forces have routinely targeted specific militant leaders for assassination, viewing them as legitimate military targets. Between 1996 and 2017, over 60 Chechen and Dagestani militant leaders were directly targeted for assassination in the North Caucasus. That is the largest number of Russian assassination operations of any category. In the rest of Russia, militants have been killed in counterterrorism operations, sometimes when terrorists have conducted hostage-taking operations, such as in the Nord-Ost theater siege in 2002 and the Beslan school siege in 2004.[458] One of Putin's early statements as prime minister in the Boris Yeltsin administration was to promise that Russia would eliminate terrorists wherever they were, even using vulgar terms regarding targeting them in their outhouses.[459] Although observers outside Russia have criticized the Russian government's heavy-handed response to terrorist attacks inside its borders, this stance was one of Putin's initial attractions for the Russian people.

External Assassinations

Assassinations outside Russia are less common than equivalent operations inside Russia probably because they are potentially more politically damaging to Russia and must be conducted more carefully. By definition, state-sponsored assassinations outside the state's own borders are covert operations.

The prominence that Russian covert assassinations have received outside Russia depends on the country-venue's willingness to openly criticize Russia: a covert assassination in the United Kingdom, for example, is more likely to receive public attention than a covert assassination in Turkey or Austria.

Unlike inside Russia, where the Russian government controls the environment, the hand of the Russian government in assassination operations outside Russia is supposed to remain hidden. However, Russian government involvement has often been identified in extraterritorial assassinations either because of poor tradecraft or because the Russian government intended for its reach to be known. In 2006, the Russian government adopted a new law authorizing extrajudicial killings abroad.[460] That law states:

> It is lawful to deprive the life of a person who commits a terrorist act, as well as causing harm to the health or property of such a person or other legally protected interests of the individual, society or the state in the suppression of a terrorist act or the implementation of other measures to combat terrorism by actions prescribed or permitted by the legislation of the Russian Federation.[461]

When commenting on such assassinations, Putin has disclaimed any knowledge of them, while also asserting that the victims deserved to be killed.[462] His denials are questionable.

External Political. Russia does weigh the consequences of being caught assassinating someone abroad, and political assassinations outside Russia are relatively rare. During the Cold War, the Soviet government balanced external political assassinations against possible political fallout, and operations targeted only those individuals who were deemed sufficiently problematic to justify the potential blowback. Georgy Markov, a vocal anti-communist, was probably among these. His assassination, by stabbing with a poison-tipped umbrella in London in 1978, was conducted by the Bulgarian government with KGB assistance and advice.[463]

More recently, external Russian political assassinations have been alleged, but, in each case, there are doubts about the circumstances. Russian business oligarch Boris Berezovsky's 2013 death under suspicious circumstances in the United Kingdom may fall into this category; his death was ruled a suicide, but questions remain.[464] Several suspicious shootings in the United States also raise questions of Russian involvement, such as an attack on American security analyst Paul Joyal in February 2007, not long after Joyal accused Putin of involvement in the assassination of FSB defector Aleksandr Litvinenko the previous year. Although Joyal claims the Russian government was behind his shooting, the perpetrators have not been identified, and Joyal would be a relatively unimportant target, out of character for a Russia external covert operation.[465]

According to a *New York Times* investigative article in October 2019 GRU Unit 29155 was reportedly involved in several covert actions that have become public. The article associated GRU officers from Unit 29155 with events including the suspected 2015 Emilian Gebrev assassination attempt (see below); a failed attempt to launch a coup in Montenegro in 2016, accompanied by a reported attempt to kill the Montenegrin prime minister; and the 2018 Sergey Skripal assassination attempt in the United Kingdom.[466] Members of the unit were also reportedly active during the 2014 takeover of Crimea and in destabilization activities in Moldova in 2014—other covert activities that did not involve assassinations.

The political objective behind external assassination operations usually clearly aligns with Russian foreign policy objectives. If the report of an assassination attempt on the Montenegrin prime minister is true, it would probably be related to the country's NATO accession.[467] Montenegro was formally invited to join NATO in December 2015 and was accepted into the alliance in June 2017. The coup attempt occurred in October 2016, on the same day as parliamentary elections were held in Montenegro that prepared the way for its NATO accession.

External Military. The largest category of external assassination targets are militant leaders. During the Soviet era, these could be any leader of an anti-Soviet military insurgent group, which the Soviet government viewed as legitimate military targets, such as White Army generals Aleksandr Kutepov in the 1920s and Yevgeniy Miller in the 1930s. During the Cold War, targets included Ukrainian nationalist leaders Georgiy Okolovich, Lev

Rebet, and Stepan Bandera, all of whom were residing in Germany when they were marked for assassination.[468] These victims were different from political targets because they led anti-Soviet militant movements outside the Soviet Union and were thus military targets in the Soviet calculus.

In the post-Soviet era, military targets have most prominently included Chechen militant leaders, who in Russia's assessment are all terrorists (see Figure 23). Between 2004 and 2019, at least 20 Chechen separatist leaders and their supporters have been the targets of assassination operations outside the Russian Federation, including 12 in Turkey, three in Ukraine, two in Austria, and one each in Qatar, United Arab Emirates (UAE), and Germany. Three of these attempts failed. The first Putin-era assassination of a Chechen militant took place in 2004 in Qatar, perpetrated by GRU operatives. Since 2008 FSB Alfa and Vympel special operations units were probably behind most of the operations, although supporters of Ramzan Kadyrov, who is Moscow's chosen leader of Chechnya and is accused of killing his opponents, probably targeted some of them with FSB support.

Figure 23. Chechen External Assassinations Targets in the Putin Era

2004: Zelimkhan Yandarbiyev, Chechen rebel leader; assassinated in Qatar; GRU officers arrested in Doha, Qatar

2008: Gaji Edilsultanov, Chechen military leader; assassinated in Istanbul, Turkey

2008: Islam Janibekov, Chechen military leader; assassinated in Istanbul, Turkey

2009: Umar Israilov, former bodyguard of Chechen leader Ramzan Kadyrov who accused Kadyrov of ordering torture; assassinated in Vienna, Austria

2009: Musa Atayev (aka Ali Osayev), Chechen military leader: assassinated in Istanbul, Turkey

2009: Salim Yamadayev, Chechen political leader and rival to Kadyrov: assassinated in Dubai, UAE

2011: Berg-Hazg Musayev, Rustam Altemirov, and Zaurbek Amriev, Chechen military members: assassinated in Istanbul, Turkey; one of the assassins was identified as a Russian criminal; the weapon was a type known to be used by Russian special forces

2011: Shamsuddin Batukayev, Chechen rebel cleric; assassination attempt in Turkey

2013: Medet Ünlü, Chechen rebel representative in Turkey; assassinated in Ankara, Turkey

2014: Abdullah Bukhari, Uzbek cleric; assassinated in Turkey; FSB connections to the assassins, as a favor to the Uzbekistani security service

2015: Kaim Saduyev, Chechen military commander; assassinated in Istanbul, Turkey

2015: Abdulvahid Edelgiriev, Chechen oppositionist who plotted to resume jihad on Russian territory, suspected in Moscow of having played a key role in a plot to kill Putin; assassinated in Istanbul, Turkey

2016: Ruslan Israpilov, Chechen oppositionist; assassinated in Kocaeli Province, Turkey

2017: Adam Osmayev and Amina Okuyeva, husband and wife Chechen activists; attacked in Kiev, Ukraine, but returned fire on assailants and survived; Moscow accused Osmayev of plotting to assassinate Putin; Okuyeva killed in an ambush later in 2017

2017: Timur Makhauri (aka Ali Timaiev), Chechen military leader; assassinated in Kiev, Ukraine

2019: Zelimkhan Khangoshvili, Chechen military leader who defected and supported Georgian intelligence; assassinated in Berlin, Germany

2020: Mamikhan Umarov, Chechen political activist and blogger; killed in Austria

Sources: Figure created by author from multiple sources, including "Russia Assassinated at Least 13 Chechens Abroad Before Victim Returned Fire in Kyiv," EuroMaidan Press*, June 21, 2017,* http://euromaidanpress.com/2017/06/21/russia-assassinated-at-least-14-chechens-abroad-before-it-failed-on-osmayev/*; "Have Russian Hitmen Been Killing with Impunity in Turkey?,"* BBC*, December 13, 2016,* https://www.bbc.com/news/magazine-38294204*.*

Syrian militant leaders have frequently been the targets of Russian military operations inside Syria. Additionally, at least four Ukrainian military leaders have been assassinated inside Ukraine, probably targeted by Ukrainian separatists with FSB or GRU support. Just as the Soviet Union viewed anti-Soviet insurgent leaders during the Cold War, the Russian government views these oppositionists as legitimate military targets, not political targets.

Another possible type of military assassination emerged when the Czech government reported in 2021 the results of its investigation into explosions at two military weapons storage sites in 2014.[469] About six months after the explosions, a Bulgarian arms dealer, Emilian Gebrev, was the target of an assassination attempt, which Bellingcat convincingly showed was conducted by GRU officers. At the time, the motive for the assassination was unclear; even Bellingcat did not attempt to assert a motivation.[470] Ukrainian officials reported in April 2021 that Gebrev was involved in acquiring the weapons that were destroyed in Czechia, and the attempt on Gebrev's life may be related to his supplying weapons to Russia's military adversary, Ukraine, or to another Russian military target, Georgia.[471] Gebrev denies any connection to arms shipments to Ukraine or Georgia.[472] However, if the reports are true, this appears to be a case of multiple converging Russian covert operations—seeking to destroy an enemy weapons shipment in a foreign country and to assassinate the individual responsible for selling the weapons.

External Traitors. Russian assassinations of former intelligence and state security officers are a special category, manifesting the Russian phrase "*бывших чекистов не бывает*" ("there is no such thing as a former chekist"). In other words, once a person is given the special trust of being an intelligence or state security officer, there is no turning back without consequences. During the Soviet era, the KGB had the mission of tracking down and neutralizing intelligence officer defectors. The act of neutralization could come in several forms: re-recruiting them to support Soviet interests; kidnapping or luring them back to the Soviet Union to face justice; or, in the most extreme cases, assassinating them.

The KGB monitored the whereabouts of defectors and approached them about returning to the Soviet Union, often using family members or friends who, under KGB direction, wrote letters imploring the defector to come back. This was the case with Georgiy Salimanov, who defected in May 1950 but was lured back to Soviet-controlled East Germany after only three months, probably with the assistance of his German girlfriend. He was executed in 1952.[473] A series of young defectors in the early 1970s also returned to the Soviet Union after only a short time in the United States, although it is unclear whether they did so on their own or were induced to return. Either way, redefection could be a major propaganda victory. According to KGB defector Oleg Kalugin, the KGB attempted to persuade Alexander Orlov to redefect for propaganda purposes in 1969, although Orlov refused.[474]

Just as desirable as luring defectors back to the Soviet Union was to re-recruit them, either through coercion using family members still in the Soviet Union, or by convincing them that their life in the West was not as meaningful as it would be if they were working for the Soviet Union. A re-recruitment operation depended partially on what accesses the defector had obtained. A job in certain high-priority organizations drew special efforts to attract a defector to work for the Soviet Union again. This was the case with a small number of intelligence office defectors, like Aleksandr Kopatskiy, who, after defecting during World War II, was re-recruited as a penetration of the CIA in Germany in the late 1940s.[475] Yuriy Pyatakov, who defected in 1966 and took the name Yury Michael Marin in the West, was re-recruited after he began working at Radio Liberty in Germany. Pyatakov later redefected, along with a series of other Radio Liberty employees from Eastern European countries.[476]

Assassinations of intelligence officer defectors were typically the last resort, reserved for the most damaging and vulnerable individuals. Representative examples include Vladimir Nestorovich (assassinated in 1925), Georgiy Agabekov (disappeared in 1937, presumed assassinated), Ignace Reiss (assassinated in 1937), Walter Krivitsky (a Soviet hand is suspected in his suspicious death in 1941), Mikhail Mondich (assassination attempted in the mid-1950s), and Nikolai Khokhlov (assassination attempted in 1957). Although it is not always obvious why a particular intelligence officer was targeted for assassination, some defectors had been particularly damaging to Soviet intelligence operations. Khokhlov, for example, exposed Soviet assassination operations when he defected in 1954. After several KGB assassinations became publicly known, especially through revelations by Khokhlov and Bogdan Stashynsky, another KGB assassin who defected in 1961, the Soviet leadership was more careful about approving assassinations, focusing only on the most damaging targets. Oleg Kalugin claims to have proposed in the 1970s the assassination of two KGB defectors from the 1950s, but the KGB leadership did not approve them. He writes that KGB Director Yuriy Andropov told him: "Leave these geezers alone. Find Oleg Lyalin and Yuri Nosenko and I will sanction the execution of those two." The KGB did not locate them, and interest in their execution eventually faded.[477] In some cases, defectors' prominence was actually their salvation, since it would be harder to target a well-known person without the Soviet hand being revealed.

Assassination operations targeting intelligence officer defectors have occurred twice in the post-Soviet era: in 2006 against former KGB/FSB officer Aleksandr Litvinenko and in 2018 against former GRU officer Sergey Skripal. UK investigators identified FSB officers involved in the Litvinenko operation,[478] and the UK government and Bellingcat identified GRU officers involved in the Skripal operation.[479] The Russian government may have played on the fear of assassination in 2019, when Russian press identified the city in which Oleg Smolenkov, a Russian who had defected in 2017, was residing in the United States.[480] Smolenkov's status as an intelligence officer is not confirmed, but the Kremlin aide did allegedly have high-level accesses. Coming just one year after the Skripal assassination attempt, the publication of Smolenkov's address was possibly an FSB leak to send an ominous message to Smolenkov and other defectors: we know where you are.

CONCLUSION: COVERT ACTIVITIES SUPPORT POLITICAL AND MILITARY AIMS

Russia has gained global notoriety for its covert operations, particularly since the illegal annexation of Crimea in 2014. These operations have a Soviet-era flavor, applying political warfare and assassination methods that have long been in the Soviet/Russian toolkit. Covert political operations have drawn extensive foreign media attention, giving Russia a reputation for manipulating other countries' political systems. These operations have sometimes been accompanied by covert insertions of military forces, either those directly under Russian government command or private military corporations that use military means to enforce Russia's foreign policy objectives.

That Russia's hand has so easily been established in these operations—including all three categories of political operations, undeclared military operations, and assassination operations—is an indicator either that Russia's covert tradecraft has deteriorated since the Cold War or that Russia is less concerned about hiding its responsibility. Either way, the steady stream of Russian covert activities especially since 2014 has earned Russia the reputation of ignoring international norms, punishing its rivals, and supporting pariah regimes.

SECTION III

HOW

Russian intelligence services have at their disposal a variety of platforms from which to conduct political, economic, S&T, and military collection and covert operations. These platforms divide into two broad categories: human based and technology based. The next two chapters explain those two categories.

Human-based platforms include intelligence officers dispatched under various covers depending on mission, target, and the counterintelligence environment. Technical platforms range from ground-based to satellite-based and computer-based. In many cases, these two types of platforms support each other, such as by providing SIGINT security for HUMINT operations or targeting human code clerks seeking information that will support SIGINT collection. Although modern technology has made clandestine HUMINT more challenging, Russia has clearly not abandoned or even diminished its efforts to use clandestine human officers abroad. At the same time, technical operations are becoming more prevalent in Russian intelligence collection, especially computer-based collection, although technical platforms cannot reach all of the information that Russian intelligence services desire to access. Russia, therefore, continues to use a full spectrum of platform types, at times in concert with each other.

CHAPTER 8

HUMAN PLATFORMS

Overall, HUMINT consists of three groups of people: case officers, support personnel, and agents. Russia dispatches case officers abroad under a variety of covers, and each type of cover has advantages and disadvantages, depending on the counterintelligence environment, diplomatic relationships, acceptance of or suspicion toward Russians in society, and the financial cost of placing certain types of officers abroad. The choice of which type of officer to deploy is also guided by the need for diplomatic immunity, communications channels, funding channels, ease of seeing through the cover, and access to people who possess the targeted information. Case officers need support personnel to communicate with headquarters, keep track of paperwork, and maintain vehicles and equipment. Finally, the officer cannot collect information without an agent who has placement in the right organization and access to the targeted information.

LEGAL COVER

The best known type of cover for a Russian intelligence officer is legal cover. Russian intelligence organizations use the term “legal” cover because the officer enters the assigned country through a legal process on a valid visa, albeit often under an assumed name. Thus, the term refers only to how the officer enters the country, not whether the officer conforms to host-country laws when conducting operations. Usually, an intelligence officer is covered as a diplomat, but the cover could also be as a press correspondent, a member of an international organization, a staff member of a cultural center, or a member of any other organization that has a formal tie to the Russian government.

On a few occasions, Russian intelligence services, particularly the FSB, declare an officer to a local government for liaison purposes. This occurs in countries where the Russian government sees the need to share intelligence with the host government, either for legitimate cooperation or for influence. When declared to the host government, the officer does not usually conduct clandestine operations, although he or she might spot and assess potential recruitment candidates for another officer to cultivate.

The main advantage of legal cover is that it grants diplomatic immunity, which is governed by international standards for the treatment of diplomats; that is, a diplomat cannot be put in jail or prosecuted in a court, no matter what they do. Exceptions have been made to diplomatic immunity in rare cases when a diplomat is involved in an extreme crime, like vehicular homicide. But even in such extreme cases, both governments must agree to the exception, which is never automatic.

For a charge of espionage, governments never make an exception to diplomatic immunity. Espionage is a political crime, not a physical crime, meaning that one country does not necessarily accept another country's definition or allegations of espionage. Additionally, because the country whose officer is conducting espionage benefits from that activity, no country will allow one of its diplomats to be prosecuted for espionage. The only recourse that remains to a host government is to declare a diplomatically covered intelligence officer persona non grata, or to expel him or her for "activities incompatible with diplomatic status." The officer is removed from the country but is not put in jail first, and no court case ensues. Sometimes an officer expelled from one country can appear in another country as a diplomat if the two host countries do not share information about intelligence officer identifications or if the second government does not politically oppose a Russian intelligence officer operating on its territory.

Hundreds of Russian intelligence officers operating under diplomatic cover have been declared personae non gratae, sometimes publicly and sometimes quietly just between the expelling country and the Russian government. Mass public expulsions have occurred several times: in 1971, the British government expelled 90 Soviet officials and disallowed the diplomatic visas of 15 others after Oleg Lyalin, a KGB officer under diplomatic cover, defected. France expelled 47 Soviet officials in 1983 after KGB officer Vladimir Vetrov's revelations about technical collection in France. In 1986, the United States expelled over 80 Soviet officials to protest the recruitment of several U.S. citizens arrested in 1985 for espionage, plus 50 more Russian officials in 2001 to protest Robert Hanssen's espionage activities. In late 2016, the United States also expelled 35 Russian officials in retaliation for Russian meddling in the U.S. elections. About 150 Russian officers were publicly expelled from 30 countries in 2018 in response to the attempted assassination of Sergey Skripal in the United Kingdom, including over 60 from the United States. In 2021, Czechia expelled nearly 80 Russians after confirming allegations of Russian involvement in explosions at two weapons storage facilities in 2014.[481] Those mass expulsions are by far not the only ones in the past decade. Since the 2018 mass expulsions, at least Greece, Hungary, Slovakia, Germany, Lithuania, Bulgaria, and Italy have expelled Russian officers under diplomatic cover for various reasons.

Diplomatically covered officers have the advantage of natural access to many government officials, including those whose job is to determine and conduct another government's foreign and military policy—both high priority intelligence targets for Russia. This interaction opens many opportunities to seek agents with useful access, either in the host government or among fellow diplomats. Many Soviet/Russian diplomatically covered officers have recruited other countries' diplomats serving in the same foreign capital. Afanasiy Shorokhov (aka Vladimir Petrov) told Australian officials that he had targeted other diplomats in Canberra during his tenure there in the 1950s, including Indonesian, French, and Israeli.[482] More recently, SVR defector Sergey Tretyakov reported that his *rezidentura* at the Russian Mission to the United Nations in New York targeted diplomats from multiple countries in the 1990s, often for the knowledge they could provide about their countries' plans for relations with Russia or the United States.[483] These recruitments were heavily focused on political collection.

Communication between the officer and headquarters is easier for diplomatically covered officers because they can use their own government communication channels and encryption systems, as well as diplomatic pouches, without raising suspicion of the host government. Legal cover can also be less expensive, because it does not require establishing a separate reason for the officer to be in the country, such as a cover business or new cover identity.

Disadvantages include the officer's overt affiliation with a foreign government, which for some people is an inhibitor to beginning a relationship, especially if antagonistic relations exist between the two countries. Some people, often including those who work in intelligence agencies, which are an important target of Russian intelligence, have an innate suspicion of foreign government representatives, making it difficult to approach them. Diplomatically covered officers are also easier to identify, because their names are published in diplomatic protocol lists. Some countries immediately assume that a foreign diplomat is an intelligence officer, especially Russian diplomats, until they can prove otherwise. Russia operates the same way, assuming that foreign diplomats posted to Russia are intelligence officers. Monitoring the finite number of foreign diplomats is easier than watching everyone who enters the country.

Sometimes, when relations between countries are particularly tense, a government will impose a travel restriction on accredited diplomats, meaning that diplomats are required to ask permission to travel beyond a certain radius around the city where they are assigned. In addition to limiting foreign diplomats' ability to visit restricted areas, this constraint makes surveillance of their movements easier. During the Cold War, Soviet diplomats had a 25-mile travel radius around their assigned cities in the United States; U.S. diplomats were similarly restricted in the Soviet Union.

Probably the biggest strategic disadvantage of diplomatically covered officers is that, if diplomatic relations are severed, the host government will expel all diplomats of the affected country. Should this occur during wartime, when intelligence is most needed, it would leave no diplomatic positions under which to cover intelligence officers. A different type of officer who can remain in place is required during periods of extreme tension, like wartime.

NONOFFICIAL COVER

Nonofficial cover (NOC) means an individual is sent abroad using legal immigration channels but without official government affiliation. A Russian NOC officer often represents a Russian entity of some kind, although not the Russian government itself. Cover might be as a banker, businessman, student, researcher, or representative of the Russian Orthodox Church, or any other position that allows for legal travel.

NOC officers, or NOCs, have the advantage of being able to enter different social circles than diplomats or formal government representatives can. They may develop relationships with other businesspeople who have access to economic or technological information or may exploit common interests to be introduced to individuals with access to military or political information. NOCs are harder to identify because they enter a country with the regular flow of foreigners, not with special diplomatic or official visas.

The disadvantage has been manifested in several cases over the past decade: NOCs can be arrested and prosecuted for espionage or for conducting foreign influence campaigns because they do not enjoy diplomatic immunity. Russian NOCs have been compromised in several locations. In 2010, a Russian businessman was arrested in Poland after living there for about 10 years and running a company that sold hunting equipment, including optical sights for hunting rifles. He reportedly developed close relationships with Polish military officials who were also hunting enthusiasts. The Polish government alleged that his company had been established with GRU funds as cover for the officer's intelligence activities.[484] He was initially referred to in the media as an illegal, but he was probably a Russian NOC instead, as he was openly living as a Russian national. In another example, Yevgeniy Buryakov arrived in the United States in 2010 as an employee of the Russian bank, VneshEconomBank; he was handled by SVR officers posted under diplomatic cover at the Russian UN Mission.[485] These two Russian NOCs were working in long-term assignments in their target countries when they were arrested. Not as many NOCs have been identified publicly as other types of officers because they may travel on short-term TDY assignments and are thus not visible for extended periods.

ILLEGAL COVER

The Soviet Union established the illegals program in 1922, primarily because the Bolshevik regime had not obtained diplomatic recognition by any country in the world to that point. Legally covered intelligence officers were not a possibility because there were no Soviet embassies. According to SVR Director Sergey Naryshkin, speaking in 2017 about the illegals program: "The concern at the time was about the very existence of the RSFSR [Russian Soviet Federated Socialist Republic]. The political and military leadership needed foundational information about enemies' plans."[486] Illegals were sent abroad without any connection to the Bolshevik regime, which was raising suspicion throughout Europe and Asia for its support for revolutions. This supposed separation from the Soviet Union provided the opportunity to gain information on "enemies" who were seen as intent on attacking Russia.

These officers are called *нелегал* (illegal) because they enter a country using false documents in a fictitious name. They typically present a persona that is completely different from their real identity. Their assumed identity is usually not Russian and has no overt connection to Russia at all.

Russia chooses illegals from two broad pools of people: Russian natives and non-Russians. Each group has advantages and disadvantages. If one of the goals of an illegal is to portray someone who is not Russian, then non-Russians start with an advantage. They can naturally portray a non-Russian in language, culture, mannerisms, and often in their experience abroad. Non-Russians do not need as much training and can portray a non-Russian without as much risk of compromise. Over the years, Soviet and Russian services have chosen numerous non-Russians as illegals from among the many nationalities of people who have emigrated or traveled to the Soviet Union. Some famous illegals have come from among this pool of people, such as Walter Krivitsky, who was born as Samuel Ginzberg in what was then the Austro-Hungarian Empire; Richard Sorge, who was German; the person known as Rudolf Abel, who was actually William Fisher from England; Morris and Lona Cohen, who were born and raised in the United States and became Soviet officers in the 1940s; and a woman named Afrika de las Heras, who was from a Spanish enclave in Morocco and lived for over 20 years as an illegal in South America. A comparable non-Russian pool of illegals and prospective illegals exists today. Russia has access to large non-Russian populations among the many individuals who travel to Russia from former Soviet republics for jobs. Russian services can easily choose candidates from among these individuals to become illegals.

The disadvantage of non-Russian illegals, however, is that they do not have the same level of loyalty to Moscow as Russian natives do. Although there have been some deeply loyal officers among this non-Russian group, non-Russian illegals have been more inclined to defect than Russian natives. The first Soviet illegal to defect, Aleksandr Sipelgas, was ethnically Estonian and was sent to Finland as an illegal in the 1920s.

Russian-ethnic candidates have just the opposite advantages and disadvantages—they take longer to train, but they are less likely to defect. Russia-born individuals are selected for illegal positions for a variety of reasons. Some possess a special skill or ability that Russian intelligence services need for operational purposes. They may have studied and shown particular aptitude for a foreign language or exhibited valor or clandestine skills during war or in internal operations. This was the case with Yevgeniy Khokhlov, who operated behind German lines during World War II and became an illegal in the 1940s. He was said to have been able to pass easily as a German.

Illegals candidates may be Russians with family connections abroad around which they could build an identity. Alexander Kouzminov, an illegals-handling officer who defected in the 1990s, described a number of illegals who were born into Greek families in the Soviet Union but who connected with relatives in Greece when they were dispatched abroad as illegals. Soviet intelligence also sought particular areas of expertise beyond foreign language capability. Kouzminov, who was responsible for handling agents who could report on biological weapons programs, visited Soviet universities looking for promising candidates with degrees in biological sciences.[487]

Whatever the qualification, a person does not volunteer to be an illegal. A volunteer would appear to be too eager and may have ulterior motives. A Russian intelligence service invites promising candidates to be illegals and, even then, puts them through rigorous testing and training to determine whether they possess the required characteristics of loyalty, courage, and ability to think independently. Russian-born illegals require much more training to be able to portray someone other than who they really are, usually undergoing years of language and cultural training so they can plausibly portray a non-Russian identity. One German agent, Hede Massing, claimed that she was tasked to meet Russian officers traveling through Germany en route to foreign assignments and "attempt to rub off some of the obviously Russian characteristics" so they more could successfully fit into Western society.[488] The Soviet services often sought Russian candidates who had lived abroad and already had at least the beginnings of an education about how non-Russians lived, although these individuals were difficult to find during the Soviet era, when the Soviet government prevented most citizens from traveling abroad.

More than anything else, an illegal needs to operate independently and remain loyal while being surrounded by people and ideas that may be opposed to the illegal's mission. Russian-born illegals have proven themselves to be more loyal than non-Russians, and few among them have chosen to defect. Most of the illegals arrested in the United States in 2010 were trained Russians. One of them, Yelena Vavilova, published a fictionalized book in 2019 that presented an autobiographical portrayal of the selection, training, and handling of illegals in Belgium, Canada, and the United States.[489]

Russian services today are experimenting with a new breed of illegals who are Russian ethnically but who do not try to portray another nationality, as seen among the group of illegal officers arrested in the United States in 2010. Three of the illegals identified at that time were young Russians who did not try to hide their Russianness, but who were handled using traditional illegals tradecraft. The SVR may have experimented to see whether, in an era when Russians can travel freely around the world, they could operate as Russians without raising suspicion. In a tradeoff that the SVR may have made to conduct its experiment, these illegals were less trained in clandestine tradecraft, so they were not as capable of keeping their missions secure.[490]

Regardless of the pool from which an illegal comes, those who persevere often become heroes. Illegals have been recognized as Heroes of the Soviet Union or Heroes of the Russian Federation, including a group of seven illegals whose identities were made public in January 2020.[491] Vladimir Putin has openly been a great supporter of the illegals program, stating in 2017, "Not everyone can deny themselves their current life, give up friends and relatives and leave the country for many, many years, and devote their life to serving the Fatherland. I say that without any exaggeration. But illegal intelligence officers live with such an approach to work, with such an approach to country and towards their people. They are unique people."[492] Putin further noted that year that he had handled illegals operations himself during his one foreign assignment as a KGB officer in Dresden, Germany. The Russian government has used that high-level advocacy to its advantage, creating an aura of greatness around illegals that makes them seem to be the highest form of intelligence. A Russian writer on intelligence topics claimed in 2017 that Western countries look with envy at Russia's illegals program and wish they had something like it.[493]

From 2000 to 2010, the United States had an unusual opportunity to observe illegals in action. In 1999, the CIA recruited an SVR officer named Aleksandr Poteyev, who worked in Department S, which runs the SVR illegals program. Poteyev provided information that led to the identification of numerous individuals who were operating as illegals around the world. Most of those illegals whose identities have been made public were either operating inside the United States or traveled to the United States, although others were in Germany and Spain. The FBI monitored their activities for 10 years in an operation codenamed *Ghost Stories*, through which the FBI collected detailed information about their targets, communications, funding, and cover lives. The illegals consisted of four married couples who arrived in the United States at various times from the late 1980s to the early 2000s and three unmarried individuals who arrived between 2006 and 2009. The officers also included one individual who occasionally traveled to the United States to support the resident illegals.[494]

Ten of these illegals were arrested in the United States in June 2010 and subsequently traded for four Russians who had cooperated with U.S. and British intelligence and were serving sentences in Russian prisons. Another was arrested on an international warrant in Cyprus, but he skipped bail and disappeared. Yet another worked at Microsoft Corporation in Washington state and was detained on an immigration violation and deported.

After the arrested officers returned to Russia, several of them received awards for their service as illegals. One of them, Mikhail Vasenkov, was among the seven illegals recognized publicly in 2020.[495] Andrey Bezrukov became prominent in Russia for running a political consulting company that provides information about the United States based on his more than 15 years living there. As noted above, Vavilova published a book that provided details about her and her husband's time in Belgium, Canada, and the United States as illegals. Anna Chapman has become a celebrity in Russia and hosts a TV show about mysteries of the world, which reveals and advances conspiracy theories.

Three of the illegals arrested or deported in 2010 (Anna Chapman, Mikhail Semenko, and Aleksey Karetnikov) represent the new trend in illegals operating as Russians. These three traveled abroad under real Russian identities and did not try to hide their Russianness while they operated. However, they were handled as illegals through clandestine and impersonal communications and by receiving funds from Moscow clandestinely, etc.[496] These three illegals arrived in the United States between 2006 and 2009, and all were young Russians in their 20s. Although they may mark the beginning of a new type of Russian illegal, their arrests and public compromise may also give the SVR some concern about their effectiveness.

Within the year following the arrests in the United States, illegals operations in at least two other countries were also compromised and ended: an individual named Sergey Cherepanov suddenly departed Spain in 2010, and a married couple, known publicly as Andreas and Heidrun Anschlag, was arrested in Germany in 2011. According to an investigative journalist, Cherepanov was pitched on the same day that the *Ghost Stories* subjects were arrested in the United States, although he refused the pitch and disappeared.[497] The Anschlags were running a Dutch diplomat, Raymond Poeteray, who had access to EU and NATO political information (see Chapter 4).[498]

Some observers have downplayed the usefulness of the illegals arrested in 2010-11, claiming that they were bumblers who accomplished little. British journalist Gordon Corera, in his book *Spies Among Us*, quotes an SVR officer who even wondered about the return on investment for illegals.[499] But the FBI's decade of monitoring the illegals revealed that they were getting close to their objective of penetrating sensitive circles. Semenko had finished a master's degree and was seeking a job in Washington policy think tanks. Lidiya Guryeva had made the acquaintance of Alan Patricof, a friend of Secretary of State Hillary Clinton. Mikhail Kutsik and Natalya Perevezeva had moved to an apartment near the Pentagon, where many of their neighbors held sensitive government positions. Yelena Vavilova claims she and her husband were beginning to cultivate valuable contacts, including an assistant to President Barack Obama.[500] Andrey Bezrukov was developing an acquaintance affiliated with George Washington University, who might have been able to recommend students aspiring to government jobs. On the West Coast, Aleksey Karetnikov was already working at Microsoft Corporation.[501] Outside the United States, illegals had made even more progress: the Anschlags in Germany were already running Dutch diplomat Raymond Poeteray and Sergey Cherepanov in Spain may have made contacts in NATO.

The French magazine *Le Nouvel Observateur*, citing information from France's counterintelligence service, the General Directorate for Internal Security, claimed in 2014 that 10 to 20 Russian illegals were operating from French territory based on intercepted clandestine radio signals.[502] These Russian operatives apparently continued to operate even after the arrests and public exposure of illegals in 2010 and 2011 in the United States and Germany.

AGENTS

Human intelligence operations cannot proceed without agents. An agent is not a member of the intelligence service, but someone the intelligence service has recruited as a source of information. Only infrequently are officers the actual sources of information. Case officers usually handle someone else who is the source. Nevertheless, officers and agents are often confused in popular media, especially when officers are called agents.

Russian services, like any HUMINT service, seek agents with placement, which means the agent occupies a potentially useful position, and access, which means the agent can gain valuable information. To recruit an agent, the officer uses his or her cover position to identify, or spot, people with placement and access who have exploitable vulnerabilities that a case officer can use to persuade the agent to cooperate.

The officer's cover allows him or her to join the circles where interaction with people of potential interest is possible. Such opportunities might include the diplomatic circuit, military-to-military engagements, think tank events, business events, trade shows, military exhibitions, sports clubs, and consular interviews. Yuriy Rastvorov, a Soviet MVD officer who defected in 1954, joined the Tokyo Lawn Tennis Club so he could make acquaintances with foreign diplomatic personnel in an informal environment.[503] Vladimir Rezun (pen name Viktor Suvorov) wrote about an operation where he and his fellow GRU officers targeted vendors at a telecommunications trade show.[504] Mikhail Repin circulated in think tanks and among political consultants from 2009 to 2011.[505] Rastvorov, Rezun, and Repin were all under legal, diplomatic cover. Yevgeniy Buryakov, a nonofficial cover officer, interacted with businessmen and bankers from 2010 to 2015, based on his cover as a banker, and he attempted to target university students who might eventually obtain positions of influence, although he reported little success. Illegal officers offer even broader circles of acquaintances through their covers as photographers, artists, businessmen, journalists, seamstresses, political consultants, students, and real estate agents, etc. Whatever the target, the circles in which the officer operates must be natural for the cover position.

Volunteers pose a different set of challenges. If a person volunteers to an intelligence service and offers to become an asset, the service's first step is to check the person's bona fides to make a preliminary determination of whether to follow up on the offer. Volunteers are risky because they can be double agents or frauds. Thus, Russia often initially suspects volunteers of being provocations unless their placement can be sufficiently confirmed and the information they offer is of sufficient quality that a foreign counterintelligence service would not likely approve it as passage material. Despite this caution and the effort Soviet and Russian officers put into spotting potential agents, many of the U.S. assets that the Soviet Union ran during the Cold War began as volunteers. These assets included most of the people who provided information about U.S. intelligence and security services, such as Aldrich Ames and Edward Lee Howard (CIA), Robert Hanssen (FBI), Christopher Boyce (NRO), William Martin and Bernon Mitchell (NSA), and John Walker (Navy cryptological information). Other American spies who did not volunteer themselves were often recruited not by a Soviet or Russian intelligence officer, but by a friend who had previously volunteered.

Use of Non-Intelligence Personnel

Russia also recruits Russian personnel who are not staff officers of a Russian intelligence service, but who are abroad as representatives of a non-intelligence organization: as diplomats, as private Russian citizens, or sometimes as religious representatives of the Russian Orthodox Church. During the Soviet era, the KGB expected non-intelligence diplomats to support intelligence tasks and provide information to the intelligence services if approached. Some "clean" diplomats bristled at this requirement, and a few decided to reject it outright. However, many cooperated, sometimes working after hours for their unofficial intelligence taskings after working all day fulfilling their regular duties.

A young Soviet diplomat named Aleksandr Kaznacheyev was unusual in the Soviet government as a proficient Burmese linguist, and the KGB *rezidentura* in the embassy in Rangoon recruited him as a translator, since none of the KGB officers were as proficient as he was; he defected to the U.S. Government in Burma in 1959. Although Kaznacheyev was not a KGB officer, he was included in KGB operations while in Burma, and he published a book in 1962 detailing Soviet influence activities in Southeast Asia. Kaznacheyev claimed in his book that, when his Burma assignment ended, he was to return to Moscow to formally become a KGB officer, but he chose to defect.[506] Another co-opted Russian diplomat was Arkadiy Shevchenko, a senior official in the United Nations in New York. He defected to the U.S. Government in 1978, and, in 1985, he published a book about Soviet intelligence activities at the UN.[507] Shevchenko also revealed details of the signals intercept station located on the roof of the Russian facility on Long Island, New York, during an interview in 1981 about Russian intelligence.[508]

Russia also targets private Russian citizens abroad to persuade them to support intelligence activities. The targeted Russians may travel abroad for legitimate business or they may have defected. Either way, Soviet and Russian intelligence can use them. In 1972, an Armenian KGB officer defected and brought with him a book, dated 1969, that listed the names of people who had left the Soviet Union illegally; during the Soviet era, it was illegal to leave the country without government authorization. Copies of the book had been distributed to KGB *rezidenturas* around the world to inform them of Soviet citizens in their areas of responsibility whom they should locate and target. The targeting could take several possible forms to include luring the defectors back to the Soviet Union to face justice or, in extreme cases, targeting them for assassination (see Chapter 7). The more likely KGB course of action was to target them for recruitment into intelligence cooperation, often using threats against their family members still living in the Soviet Union. The list included a broad range of people, such as journalists, teachers, merchant seamen, soldiers stationed abroad, and a few intelligence officers. In a few cases, a KGB *rezidentura* was successful in re-recruiting a defector.[509]

One such defector who was recruited abroad by the KGB was Oleg Tumanov, who jumped from a Soviet merchant ship off the coast of Libya in 1965. After a few years in the West, he was hired as a researcher by Radio Free Europe, a high-priority Soviet intelligence target whose European headquarters was in Munich, Germany. A KGB officer approached him in Germany, and he agreed to work for the KGB for over a decade until he was identified as a Soviet penetration agent in 1986 and redefected. The presence of his name on a 1969 KGB list indicates that he had not yet been recruited at that time. Tumanov also published a book about his experiences, although it appeared after his redefection and contained a heavy dose of anti-U.S. propaganda.[510]

Several instances of Russia targeting its own citizens traveling abroad have come to light in the past decade. Two young women whose cases became prominent in 2011 and 2017, Mariya Butina in the United States and Katia Zatuliveter in the United Kingdom, respectively, are probably among this kind of operative. Neither is believed to have been a staff intelligence officer, but the Russian government probably used both for their accesses, and both probably agreed (see Chapter 4). This kind of operative offers opportunities to penetrate different social circles, including the Russian émigré community to which Russia is eager to gain access. Like Tumanov, these operatives can be hired into positions where a Russian government official would never be considered; they can hide among the crowd more easily and be less visible to a host country's counterintelligence service. Butina and Zatuliveter had access to political circles without suspicion.

The disadvantage of these Russian operatives is that sometimes they cooperate out of duty or coercion, not out of a belief in their Russian intelligence tasks. They can become resentful that they are forced to fulfill tasks for which they did not volunteer, resulting in either faulty work or defection. These operatives are also not trained intelligence personnel, so it is risky to assign them sensitive tasks because they may not understand the particulars of clandestine operations and security.

REZIDENTURA ORGANIZATION

A Russian intelligence *rezidentura* is made up of various roles, from the *rezident*, who manages the office, to case officers, who conduct operations, and support personnel, who provide communications, clerical, and maintenance services:

- ***Rezident,*** the chief of a Russian intelligence *rezidentura,* is supreme in his domain. He is the main contact between the *rezidentura* and headquarters in Moscow and thus has a great deal of political authority among the case officers.

- **Deputy *Rezident*** runs the day-to-day affairs of the *rezidentura*. One such deputy was Sergey Tretyakov, an SVR officer who defected in 1999 and described his role as including covering for a *rezident* who was politically connected but operationally incompetent.
- **Case Officers** are divided within an SVR *rezidentura* into "lines" according to their specialization (see Figure 24). The number of officers in each line varies depending on the *rezidentura*. These beginner- to mid-level officers run the operations of the *rezidentura*.

Figure 24. Officer Lines Within an SVR *Rezidentura*

Line PR: Political intelligence, the largest portion of most *rezidenturas*

Line X: Scientific and technical intelligence, large in some *rezidenturas* where S&T information is especially accessible, such as at the former San Francisco consulate

Line N: Support to illegals, tasked with identifying dead drop sites, supporting the delivery of instructions and funds, and collecting information to support the development of legends (birth and death information; forms and requirements to support legalization)

Line KR: Counterintelligence and security, responsible for penetrating local security services

Line SK: Security and surveillance of the Soviet diplomatic community, responsible for monitoring Russians abroad

Line EM: Intelligence on émigrés, a Cold War-era function to penetrate émigré communities

In addition to these case officer roles, *rezidenturas* also require a variety of support personnel to maintain operational readiness and security:

- Code clerks encrypt and decrypt communications between headquarters and the *rezidentura*. Several code clerks defected during the Soviet era, including Igor Gouzenko in Canada in 1945 and

Yevdokiya Kartseva (aka Petrova) in Australia in 1954. Code clerks have access to nearly all of the *rezidentura*'s communications, making them lucrative targets for recruitment. Russian intelligence services also target code clerks, and several people who were the U.S. equivalent—such as James MacMillan in Moscow in 1948 and John Walker (1968–85)—defected to or spied for the Soviet Union during the Cold War and caused significant damage (see Chapter 9).

- Secretaries keep track of files and personnel. As defectors, they also can be the source of valuable intelligence, as was Raya Kiselnikova who defected in Mexico City in 1970.
- Electronic surveillance monitors (Line OT) scan local counterintelligence radio traffic to determine whether an officer is under surveillance. This radio monitoring differs from strategic SIGINT collection (see Chapter 9).
- Radio operators assigned to illegal *rezidenturas* maintain communications with headquarters on behalf of their *rezidents*. In other situations, an illegal conducts his or her own radio communications or—if deployed in a pair, such as a husband and wife—one will be the communicator.
- Personnel to maintain computers (Line I)
- Drivers/auto mechanics are responsible for one of the potentially most identifiable pieces of equipment that an intelligence officer uses, a car. The car can also become a tracking device if a local counterintelligence service can emplace a tracker in it. A driver/auto mechanic keeps the cars running, drives securely to avoid surveillance, and monitors the vehicle to ensure it is free of tracking devices.

CONCLUSION: HUMINT OPERATIONS REMAIN ESSENTIAL

Russian intelligence services, particularly the SVR and GRU, rely heavily on HUMINT operations worldwide, using all three types of covers—legal, nonofficial, and illegal—to access information that technical collection systems cannot reach. Although modern technology has made clandestine HUMINT operations riskier and more difficult, Russian leaders, including Vladimir Putin himself, continue to heap public praise on Russian intelligence officers.

Illegal cover is particularly affected by technologies that secure borders and identify travelers. However, the foundational reason for Russian illegals—the need to retain an intelligence presence even when legally covered officers cannot operate as freely—still exists. Since 2014, Russian diplomatic relations have suffered numerous setbacks, leading to hundreds of legally-covered Russian officers being expelled from countries around the world. The United States leads in the number of those expulsions, with over 100 Russian officers forced to leave since 2016, and four diplomatic establishments in the United States closed. Even countries that are typically seen as friendly to Russia, such as Greece, Austria, and Hungary, have expelled Russian officers. Tense diplomatic relations have also led to increasingly hostile counterintelligence environments for Russian services. Illegals continue to be a tool that Russian intelligence services use, despite public exposures and embarrassments.

As in the early Bolshevik days, the Russian government still sees enemies attacking Russia from all sides, now especially from the United States and NATO. With Putin's personal support, Russia is not likely to reduce its emphasis on HUMINT operations, which have brought much success in the past, are the object of much pride and adulation, and remain necessary in an uncertain world.

CHAPTER 9

TECHNICAL PLATFORMS

The second major category of collection platforms includes those that acquire information through technical collection systems rather than directly from humans. Russian technical collection comes in three primary forms: SIGINT, geospatial intelligence (GEOINT), and computer-based collection (often called cyber). These collection capabilities support all intelligence operational areas: political, economic/S&T, military, and covert operations. They are also connected to and cooperative with HUMINT, sometimes through the recruitment of foreign personnel who have access to code and cipher material, which facilitates SIGINT collection, or through intelligence officers' clandestine travel to locations around the world to conduct close access technical operations.

Russian SIGINT collection can be divided into six main platform types:

- Ground-based in Russia or in Russian-controlled territory
- Embassy-based
- Close access
- Sea-based
- Airborne
- Satellite-based

The GRU exclusively runs several of those platforms (sea-based, airborne, and satellite-based), and they focus predominantly on military intelligence and combat support. The GRU also controls Russia's space-based GEOINT system that provides optical and radar imagery, cartographic imagery, and infrared early warning capabilities; GEOINT is derived from analysis of images and data associated with a particular geographic location. Global media have publicized numerous Russian-sponsored computer-based collection operations. Much information about that collection capability can be derived from the vast number of attributed cases.

SIGINT

During the Cold War, several Soviet officers who had SIGINT experience defected to the West and shared their critical knowledge about Soviet SIGINT capabilities and targets (see Figure 25). Although post-Soviet Russian SIGINT has gone through several organizational changes (see Chapter 2), the basic forms of Russian SIGINT collection remain similar to those of the Cold War Soviet era.

Ground-based SIGINT

The Soviet Union established an extensive ground-based SIGINT collection and direction-finding capability. Most of that capability, and the largest element of the Soviet Union's SIGINT establishment overall, was inside the former Soviet Union. The GRU's Sixth Directorate operated some of these facilities, and various KGB elements ran others. The KGB conducted civilian intelligence collection and counterintelligence operations, including electronic penetrations of foreign embassies and monitoring of Soviet citizens' communications for dissent and foreign connections. Foreign intelligence communications intercepts and communications security were both managed by the KGB Eighth Chief Directorate until 1972, when the KGB created a new directorate, the Sixteenth, called *Радиоэлектронная разведка* (Radio-electronic Intelligence), which took responsibility for

Figure 25. Cold War-era SIGINT Defectors

Yuriy Rastvorov worked in a Japanese decryption unit in the Soviet Far East in 1943–44. He defected in 1954.

Yevdokiya Kartseva (aka Petrova) worked as a Russian SIGINT translator from the 1930s to 1942. She was assigned to the Japanese section in an NKVD unit responsible for decrypting the codes used by foreign diplomatic missions in Moscow. Kartseva defected in 1954 in Australia.

Ivan Ovchinnikov was a junior officer in the Group of Soviet Forces Germany (GSFG). He provided useful information on the Soviet military and GRU intercept operations and activities, as well as the mission of the KGB signal battalion in Stanhnsdorf, East Germany, which monitored official radio traffic of the Allied military and foreign diplomatic transmissions. Ovchinnikov defected in 1955 but re-defected to East Germany in October 1958; he published a book in 2000.

Yuriy Pyatakov jumped from the Soviet intelligence collection ship *Deflektor* in 1966 off the west coast of the United States. He resettled in the United States; however, he was contacted by the KGB and recruited as a source. Pyatakov later worked at Radio Liberty in Munich, Germany, and redefected in 1973.

Viktor Sheymov was a SIGINT operator at KGB headquarters in Moscow until he defected in 1980. He published a book, *Tower of Secrets*, about Soviet SIGINT in 1993.

Sources: Figure created by author from multiple sources, including U.S. Army, G2, U.S. Forces Far East, “RASTVOROV, Yurii Alexandrovitch,” March 25, 1954, National Archives and Records Administration, RG 319, Entry A1 314B, Box 627; “Mrs. Petrov’s Statement Concerning Her Past Intelligence History,” May 15, 1954, National Archives of Australia, A6283, folder 14, item number 4104675, 37-41; Frank J. Rafalko, ed., CI Reader: American Revolution Into the New Millennium*, vol 3. (Washington, DC: Office of the National Counterintelligence Executive, 2004), 67-68; Ivan Vasilyevich Ovchinnikov, Исповедь Кулацкого Сына (*Confession of a Kulak’s Son*) (Moscow: Desnitsa, 2000); Richard Cummings,* Cold War Radio: The Dangerous History of American Broadcasting in Europe, 1950-1989 *(Jefferson, NC: McFarland and Co., 2009), 176-78; Victor Sheymov,* Tower of Secrets: A Real Life Spy Thriller *(Annapolis, MD: Naval Institute Press, 1993); Matt Schudel, “Victor Sheymov, KGB Officer Who Defected From Soviet Union, Dies at 73,”* Washington Post*, December 5, 2019,* https://www.washingtonpost.com/local/obituaries/victor-sheymov-kgb-officer-who-defected-from-soviet-union-dies-at-73/2019/12/05/e773a22c-16b5-11ea-a659-7d69641c6ff7_story.html.

communications intercepts and left communications security and cryptography to the Eighth Directorate. According to an assessment from the late Cold War, the Sixteenth Directorate had about 2,000 personnel in 1989 and was growing in personnel and importance within the KGB when the Soviet Union dissolved.[511] During the Soviet era, the KGB's collection of foreign embassy communications was handled jointly by the Sixteenth Directorate for intelligence purposes and the Second Chief Directorate for counterintelligence purposes.

Separate from the Sixteenth Directorate was Department Sixteen of the First Chief Directorate, which targeted foreign communications personnel and code clerks specifically. The recruitment of a foreign code clerk is always a high priority HUMINT effort, and the KGB's HUMINT directorate had an element dedicated to that specifically.[512] If an intelligence service can recruit a code clerk or communicator, that person may provide the keys to decrypt and decode his or her own country's communications, which would facilitate the intelligence service's SIGINT operations.

The Soviet Union had considerable success recruiting foreign personnel with access to codes and ciphers. The Ministry of State Security (MGB) recruited James MacMillan, a cipher clerk at the U.S. Embassy in Moscow in 1948. He defected and provided details of the code room where he worked. Others subsequently recruited by the KGB and Eastern Bloc intelligence services include John Walker, a Navy warrant officer, who provided the Soviet Union with U.S. Navy cryptographic materials for 18 years until his arrest in 1985. His materials, which covered much of the Vietnam War period, allowed the Soviets to warn the North Vietnamese about U.S. military activities, probably leading to the deaths of U.S. personnel fighting in Vietnam.[513] U.S. Air Force airman Jeffrey Carney defected to East Germany in 1985 and subsequently worked for the East German intelligence service, translating English-language materials. For him, the fall of the Berlin Wall was a crisis, as it suddenly meant he was accessible to Western counterintelligence agencies. When East German Stasi files were opened, Carney's internal file showed the value of his work for the Stasi and the KGB, earning praise from General Mikhail Zaitsev of the Group of Soviet Forces in East Germany and

KGB Director Viktor Chebrikov. Carney was arrested in Germany in 1991 and prosecuted for espionage and desertion.[514]

After the dissolution of the Soviet Union, the Russian government created the Federal Agency for Government Communications and Information (FAPSI), combining the Eighth Main Directorate and the Sixteenth Directorate into a single organization from 1993 to 2003 (see Chapter 2).[515] During that decade, Russia had a separate, dedicated SIGINT organization for the only time in its history; at all other times SIGINT has been subordinated to other intelligence or security agencies, such as the KGB or FSB. In 2003, FAPSI was dissolved as an independent agency, and most of what were previously the Eighth and Sixteenth KGB directorates were transferred into the FSB, which has assumed the KGB's earlier responsibility for electronically penetrating foreign embassy communications and global SIGINT collection. The responsibility for the security of government communications, a remnant of the old Eighth Chief Directorate, was folded into the Federal Protective Service (FSO).[516]

The GRU is responsible for military SIGINT. The GRU Sixth Directorate, or *радиотехническая разведка* (Radio-Technical Intelligence Directorate), collects military- and political-related communications intelligence (COMINT) and electronic intelligence (ELINT). During the Cold War, the Sixth Directorate ran a series of ground-based collection facilities across the Soviet Union and in other countries, some of which continue to exist today. These sites collect various types of signals, and massive high frequency direction finding sites direct the collectors toward desired signals.

The GRU also maintains vehicle-mounted mobile SIGINT sensors for tactical environments. A 2019 advertisement from a Russian high-tech company, Rostec, touts the importance of SIGINT:

> Currently, when military forces cannot function without using radio-electronic systems, SIGINT has taken on greater significance. In fact, radio-electronic emanations are the unique "handwriting" of military technology, and the analysis of them allows for a precise determination of the type of emanating entity and the nature of its

> activity. SIGINT data allows for timely warning to a commander of security threats to counter them in time.[517]

Because the company is trying to sell its product, this advertisement contains an element of salesmanship. Nevertheless, the GRU does have a tactical SIGINT mission using ground-based platforms such as the one Rostec sells, and thus is a ready buyer.

The end of the Cold War significantly limited Russia's ground-based SIGINT capability. The Soviet Union had SIGINT sites spread throughout the Warsaw Pact, especially in East Germany, to which the Russian Federation lost access when the Soviet Union dissolved. Advantageously for the West, two Cold War defectors from those units had shared their insights into Soviet SIGINT activities: one in 1948 from Soviet occupation forces in Hungary and one in 1955 from the Group of Soviet Forces in East Germany. The latter defector, Ivan Ovchinnikov, provided significant information about the organization and targets of both GRU and KGB SIGINT in East Germany. The Soviet Union had other ground-based SIGINT facilities in Soviet-allied countries around the world, including in Vietnam, South Yemen, Burma, Mongolia, and Nicaragua, as well as in Afghanistan where Soviet troops were stationed from 1979 to 1989.

The largest Soviet SIGINT facility outside the Soviet Union was at Lourdes, Cuba. The Lourdes site initially opened in the early 1960s after the Cuban missile crisis and became a point of contention in U.S.-Soviet relations. In 1983, U.S. President Ronald Reagan complained:

> This Soviet intelligence collection facility less than 100 miles from our coast is the largest of its kind in the world. The acres and acres of antennae fields and intelligence monitors are targeted on key U.S. military installations and sensitive activities. The installation in Lourdes, Cuba, is manned by 1,500 Soviet technicians [it later grew to over 2,000], and the satellite ground station allows instant communications with Moscow. This 28-square mile facility has grown by more than 50 percent in size and capability during the past decade.[518]

A joint State-Defense Department statement in 1985 assessed: "From this key listening post, the Soviets monitor U.S. commercial satellites, U.S. military and merchant shipping communications, and NASA space program activities at Cape Canaveral. Lourdes also enables the Soviets to eavesdrop on telephone conversations in the United States."[519] According to Russian author Aleksandr Kolpakidi, in 1985, approximately 70 percent of the Soviet Union's intelligence about the United States came from Lourdes.[520] Lourdes closed in 2001 when Russia was unable to continue to fund it; however, since 2014 Russian commentators have made tangential statements that the site should be reopened. The Russian government has made no formal announcement, although it has offered to return military support to Cuba, as well as to Vietnam, as provided during the Cold War.[521]

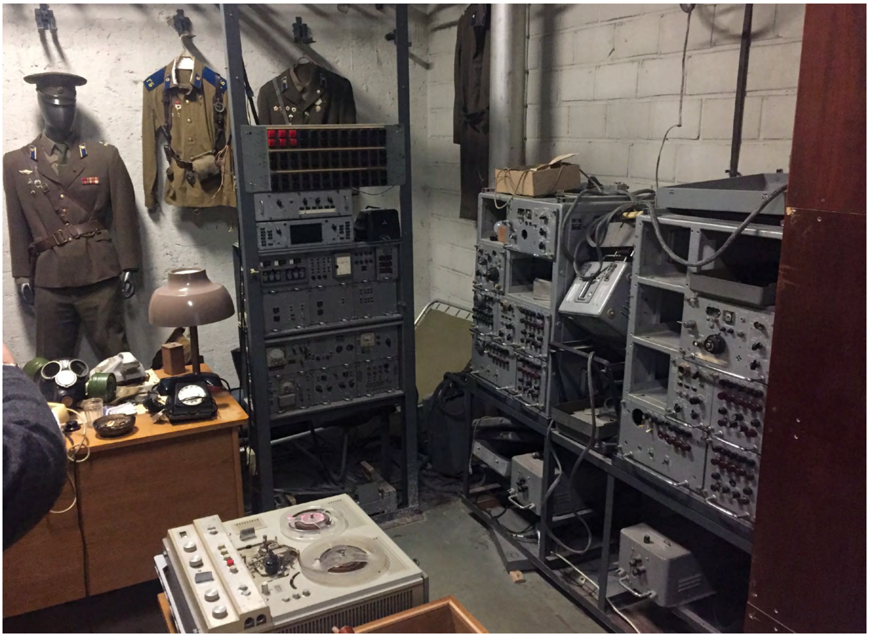
The Soviet Union also operated a series of ground-based early warning radar sites—long-distance airspace monitoring radars for ballistic missile and air defense warning—across the Soviet Union. A current system is also spread across Russia and in three foreign sites: one each in Armenia, Belarus, and Russian-occupied Crimea.[522] Russia has lost several similar radars since the dissolution of the Soviet Union, one in Latvia in 1998 and one in Azerbaijan in 2012.[523]

The GRU continues to benefit from another Cold War-era facility in Tajikistan that conducts space surveillance and monitoring of foreign satellites. The facility is called Okno, which means "window." The Okno Outer-Space Control System (Russian acronym SKKP) was upgraded in 2014 to give it the capability to detect objects in space to a distance of 50,000 kilometers. Okno is part of a complex of radiolocation and electro-optical sensors located around Russia for space surveillance, which the Russian Ministry of Defense claims offers a capability to catalogue and monitor space-based objects and maintain constant visibility on activities in space.[524]

The FSB also conducts SIGINT inside Russia, directed at foreign diplomatic facilities for both intelligence and counterintelligence purposes, similar to earlier KGB activities. The FSB has access to communications throughout Russia via the *Система оперативно-разыскных мероприятий* (System for Operational Investigative Measures), or SORM in its Russian acronym.

Through that access, the FSB can collect counterintelligence and security information, including information for counterterrorism and anti-dissident operations and for positive intelligence purposes. SORM allows access to Internet communications activity throughout Russia, and numerous oppositionists have been apprehended based on the collection of their internal communications. The FSB also has an organization called Center 16 (also called "Military Unit 71330") that collects signals for positive intelligence purposes. According to an Estonian study, Center 16 can collect radio, satellite, mobile phone, and data communications.[525] Like the KGB before it, the FSB controls Russia's information environment, and signals collection is a major part of that control.

Figure 26. SIGINT Collection Room in the Hotel Viru in Tallinn, Estonia



Source: Photo by author.

Note: The Hotel Viru was built to Western quality standards and was thus quite different from most hotels in the Soviet Union. Numerous foreign dignitaries stayed at the hotel, and the KGB wired it for SIGINT collection, both through telephone intercept and recording the personal conversations of residents. In this room, on the top floor of the hotel, KGB personnel would record the communications. This room is now a museum.

Collection from Diplomatic Establishments

A portion of Russia's ground-based SIGINT collection capability is housed in Russian embassies and other official establishments abroad. At the end of the Cold War, Russia had SIGINT facilities in over 60 countries, with multiple sites in many countries, bringing the total number of SIGINT collection platforms to about 100. These platforms were used, and in many cases continue to be used, for political, economic, and S&T collection, as well as for counterintelligence and operational security monitoring in support of Russian human operations. A late Cold War estimate counted over 1,000 Soviet SIGINT personnel working at these facilities.[526] The number of embassy-based SIGINT facilities probably dropped after the dissolution of the Soviet Union but, judging from other Russian intelligence activities, SIGINT facilities have probably returned to or exceeded their Cold War level during the Putin era. These sites house GRU and SVR SIGINT collection capabilities.

Materials from KGB defector Vasiliy Mitrokhin indicate that the KGB installed the first embassy-based SIGINT platform in Mexico City in 1963, targeted primarily at the U.S. Embassy and CIA Station in the city. Although Mitrokhin claimed that the platform was not particularly successful at that point,[527] the effectiveness of embassy-based SIGINT platforms apparently improved over time. As Oleg Kalugin, a KGB officer who worked in Washington, DC, from 1965 to 1970, wrote:

> In 1967, we placed antennas on the roof of our embassy and suddenly we were able to overhear the communications of the Pentagon, the FBI, the State Department, the White House, the local police, and a host of other agencies... Transcripts of the conversations, when compared with classified sources of information at our disposal, enabled us to piece together everything from the secretary of state's travel schedule to the latest crimes being investigated by the FBI.[528]

Until 2016, at least four such facilities were operating inside the United States. The U.S. Government had a rare opportunity to get an inside look at a SIGINT collection facility in 2016, when the United States ordered

Russia to close its San Francisco Consulate and Russian-government owned recreation facilities in New York and Maryland. The San Francisco Consulate was well-positioned for line-of-sight SIGINT collection of much of the San Francisco Bay area, and it housed an assortment of antennas on the roof. A 2017 article by journalist Zach Dorfman quoted a U.S. official as saying, "It was almost like everyone they had there was a technical guy."[529] Russian diplomatic compounds in Maryland and New York had a similar purpose. Arkadiy Shevchenko, a Soviet diplomat who defected in New York City in 1978, claimed that the top floors of the Soviet embassy residential compound in the Bronx, New York were "full of sophisticate equipment... to intercept all the conversations on anything which was going on. At least 15 to 17 technicians were working to do all this job [*sic*]."[530] An equivalent compound on Maryland's Eastern Shore, closed in 2016, was also used for intelligence purposes. According to a U.S. official, the New York and Maryland compounds were "basically being used as signals intelligence facilities."[531] In addition to those compounds, the new Russian embassy compound, situated on one of the highest points in Washington, DC, has line-of-sight access to much of the DC area, including about five-mile, line-of-site visibility directly onto the Pentagon. Completed in 1985, its roof is also covered with antennas,[532] similar to Kalugin's description above of the earlier Soviet embassy.

Kalugin asserted that the KGB used these facilities for political collection. A Canadian documentary produced in 1981 also indicated their use for economic collection. The documentary claimed that conversations intercepted from the Soviet embassy's SIGINT platform in Washington, DC, gave the Soviet government the upper hand when the United States and the Soviet Union were negotiating a grain sale in 1972.[533]

SIGINT facilities such as these require the ability to both intercept and interpret the signals. Kalugin noted that the Washington KGB *rezidentura* had the in-house capability to fuse HUMINT and SIGINT to improve targeting and provide a complete intelligence picture.[534] That capability may not be at every facility—Australian defense expert Desmond Ball wrote in 1989 that SIGINT facilities in Washington and New York sent materials to Lourdes, Cuba, for processing, while most facilities sent materials to

Moscow to be interpreted and reported.[535] The advent of large-volume digital communications has probably made the fusion of different intelligence streams faster and easier.

Another focus of this SIGINT collection is the signals of U.S. counterintelligence surveillance teams. Special technicians in SVR Line OT perform this function, which intelligence writer Nigel West has referred to by the Russian code names *Impuls* and *Zenit*.[536] Mitrokhin reported that the KGB *rezidenturas* in Washington, New York, and San Francisco all had SIGINT posts, for which he used the code name *Raketa*, whose responsibility was to provide "a picture of the operational environment and the FBI's conduct of operations… if necessary an operations officer can be given a danger signal prior to his going out to the site when an operation is to be conducted, [or told] to back off from an operation if he has been detected by surveillance."[537] KGB defector Sergey Tretyakov described using what he called the *Impulse* signaling system to avoid surveillance during his time in New York.[538]

In 2019, U.S. journalists revealed a Russian program that targeted FBI surveillance communication, which provided Russian intelligence officers forewarning of FBI counterintelligence activities and identified potential gaps in surveillance coverage. An SVR *rezidentura* could use this information to operate with less risk of compromise. As a U.S. intelligence official was quoted in 2019: "When we found out about this, the light bulb went on—that this could be why we haven't seen [certain types of] activity" from known Russian officers in the United States.[539]

Close Access Technical Operations

Some signals are not easily accessible remotely but can be collected more readily through direct, close access to a network. In that vein, Russia sends officers around the world, as TDY travelers or based at embassies, to get closer to the signals that Russia is trying to collect. Sometimes these operations involve emplacing, inside a building, listening devices that transmit to a receiver outside, and sometimes the operations collect emanations, like cell phone or wi-fi signals. Close access technical operations, therefore, are another example of the crossover between human and technical platforms, as Russia applies clandestine tradecraft typically used in HUMINT operations, whether for international travel or by diplomatically-covered intelligence officers, to support technical collection.

As noted in Chapter 4, Russian embassy officer Stanislav Gusev was arrested in December 1999 while sitting in a vehicle outside the U.S. Department of State building in Washington, DC. He was receiving the signals from a listening device installed in the U.S. State Department Oceans and International Environmental Scientific Affairs (OES) conference room. After Washington, DC, police observed Gusev sitting in a vehicle outside the State Department multiple times, they informed the FBI, which approached him and discovered his activity.

Several examples of close access technical collection operations have been reported during the Putin era. Four Russians arrived in the Netherlands in April 2018, and police caught them with signal intercept equipment at a hotel located next to the Organization for the Prohibition of Chemical Weapons (OPCW) headquarters in The Hague. At the time, the OPCW was testing the substance used the previous month in the attempted assassination of Sergei Skripal and his daughter Julia in the United Kingdom. The OPCW was also analyzing a chemical used in an attack in Douma, Syria, just a few days previously. The four Russians subsequently planned to travel to a laboratory in Spiez, Switzerland, that the OPCW uses to analyze chemical weapons samples.[540] The laptop of one of the officers showed that it had recently been in Brazil, Switzerland, and Malaysia. The Malaysia trip was related to the investigation of the MH17 flight; the Switzerland travel was linked to the hacking of a laptop belonging to the World Anti-Doping Agency.[541]

In September 2018, Norwegian police arrested Russian Mikhail Bochkarev for a close access SIGINT operation while attending a conference at Norway's Parliament building. Bochkarev was later released, although probably because of the sensitivity of the investigation, not because of the absence of nefarious activity, as the Russian government claimed (see Chapter 4).[542] Bochkarev was probably conducting a survey of signals in the facility and among other attendees at the event to facilitate future SIGINT collection. Then, in August 2019, Swiss police arrested two Russian men, one of whom was posing as a plumber; Swiss police and federal officials suspected the two Russians were intelligence operatives preparing to conduct electronic surveillance. The men claimed diplomatic immunity but had never officially registered as diplomats. Their travel coincided with the annual World Economic Forum, where political leaders from around the world meet to discuss major international economic and political issues.[543] These recent incidents in the Netherlands, Norway, and Switzerland all involved officers from GRU Unit 26165, dedicated to SIGINT collection, and all appeared to be for political intelligence purposes.

Additionally, as noted in Chapter 6, U.S. officials have observed Russian intelligence officers traveling to remote locations with packages in their hands or wearing backpacks, pushing strollers, or driving by in vehicles. U.S. officials have concluded that these activities are probably related to collecting intelligence on critical infrastructure sites, possibly mapping them or characterizing the signals that emanate from them.[544] If their analysis is correct, this would be related to contingency military intelligence collection in preparation for future war, in which Russia would target critical infrastructure sites as part of SODCIT.

Sea-based SIGINT

For Russia, sea-based SIGINT has primarily a military intelligence mission, monitoring foreign threat forces and supporting Russian military warning, planning, and operations. Russia maintains a fleet of as many as 60 sea-based intelligence collection platforms known as auxiliary general intelligence ships (AGIs). At least one GRU officer deployed aboard a Soviet AGI defected to the United States during the Cold War: Yuriy Pyatakov (also known as Yuri Marin) was a linguist aboard the Soviet intelligence collection ship *Deflektor* until February 18, 1966, when he jumped overboard and was picked from the water by a U.S. Navy vessel. Pyatakov was debriefed about his duties on board the SIGINT collection ship.[545]

According to Desmond Ball, Soviet-era AGIs fulfilled a series of routine missions, several of which have been observed publicly during the Putin era:[546]

- **Patrol near U.S. nuclear missile submarine bases.** Ball has noted that Soviet AGIs regularly patrolled off the coast of Rota, Spain; Kings Bay, Georgia; Apra Harbor, Guam; and Holy Loch, Scotland—all of which were U.S. submarine bases. Russia has reinvigorated this patrol operation since at least 2014. In December 2019, the U.S. Coast Guard issued a warning to ships navigating off the coast of South Carolina and Georgia due to what it called unsafe practices of the Russian AGI *Viktor Leonov*. The Russian ship was operating without lights and ignoring calls from passing ships that were trying to steer clear of it. The same ship had also been observed near Kings Bay in 2018, and probably as far back as 2014.[547]
- **Monitor naval exercises.** Soviet AGIs routinely loitered in the area of U.S. naval exercises, probably to collect command and control signals that could be used to recognize those signals during wartime, as well as to monitor U.S. naval doctrine and capabilities. More recently, in 2015 and 2016, Russian ships, including an AGI, monitored NATO exercise BALTOPS in the Baltic Sea. Russian ships had previously been invited to be overt participants in BALTOPS until the 2014 annexation of Crimea; since then, they have loitered on the margins of the exercise.[548] A Russian AGI was reported off the coast of Hawaii monitoring exercise RIMPAC 2016, although none was detected in 2020.[549] The Russian news service TASS reported that Russian intelligence collection ships deployed in reaction to NATO's Sea Shield-2019 exercise in the Black Sea.[550]
- **Monitor maritime chokepoints.** Soviet AGIs regularly patrolled in maritime chokepoints around the world looking for the passage of military vessels. Russian AGIs similarly patrol in chokepoints, such as the Sea of Japan, the Greenland-Iceland-UK Gap, and the Mediterranean Sea.

- **Shadow naval vessels during normal operations.** In 2017, the AGI *Viktor Leonov* was spotted 70 miles off the coast of Delaware, a major shipping lane for U.S. ships coming from Norfolk Navy Base. The AGI sailed on to the Connecticut coast, near the U.S. submarine base at New London.[551]

Other Soviet-era AGI missions included monitoring U.S. naval ship and missile trials to collect telemetry and communications wherever the AGI was operating. Since 2015, Russian AGIs have also rotated into the eastern Mediterranean Sea on a regular basis as part of Russian military operations in Syria. AGIs even participated in a Russian Navy Day celebration off the coast of Tartus, Syria, in 2017. That year, the Russian AGI *Liman* collided with a cargo ship in the Black Sea, as the AGI was on its way to Syria. The *Liman* was built in 1970 and was in use from then until it sank after the 2017 encounter.[552] The same ship sat in the Adriatic Sea during the NATO bombing of Yugoslavia in 1999 and monitored NATO air activity, probably to relay information to the Serbian forces. Soviet/Russian AGIs also reportedly supported North Vietnam during the Vietnam War and now support Syria in the Syria civil war.

In more modern times, Russian ships have been observed reconnoitering undersea communications cables. The Russian undersea ship *Yantar* has loitered off the coast of Florida and in the North Atlantic Ocean in areas where undersea cables are present (see Chapter 6). That technical collection, combined with human collection on the shoreline, gives Russia an accurate picture of the potential targeting locations of undersea communications infrastructures and is another example of the collaborative relationship between Russian HUMINT and technical collection platforms.[553]

Airborne SIGINT

Russia's SIGINT aircraft are mostly focused on ELINT, ISR targeting, and jamming missions in direct support to military operations. They have operated in several Russian military campaigns since 2014, particularly in Ukraine and Syria. For example, in 2015, Russia deployed its IL-20 SIGINT aircraft—the Russian air force's primary reconnaissance aircraft—to Syria. The IL-20 is an ELINT platform that is equipped with a wide array of antennas, infrared and optical sensors, a side-looking airborne radar, and satellite communication equipment for real-time data sharing.[554]

The Russian Tu-214R SIGINT collection and targeting aircraft also deployed to Syria in 2016. The Tu-214R is Russia's most modern ISR aircraft, equipped with sensors to perform ELINT and COMINT missions, and with all-weather radar systems and electro-optical GEOINT sensors. The aircraft usually loiters in uncontested airspace at high altitude and a safe distance from the targets of interest, rather than entering combat areas, and its sensors can intercept and analyze signals emitted by targeted systems (e.g., radars, aircraft, radios, combat vehicles, mobile phones, etc.) while collecting imagery that can identify and pinpoint enemy forces, even if they are camouflaged or hidden. The Tu-214R can build an electronic order of battle, which is an inventory of an adversary's electronic emitters, and communicate that information to targeters for kinetic attack.[555] One military journalist has surmised that the presence of the Tu-214R in Syria might be serving not only in support to combat operations, but also for gathering information for Russia about U.S. aircraft signals in the theater.[556]

In 2017, Russia reportedly deployed a third SIGINT aircraft—the IL-22PP SIGINT/electronic warfare platform—to Syria. The IL-22PP is an airborne electronic jammer that can detect and block all types of signals, particularly digital ones used by Western warplanes and radars like those used by AWACS aircraft.[557] In 2020, the IL-22PP was involved in an incident between a Turkish and Syrian aircraft. Reportedly, an IL-22PP jammed the targeting signals of a Turkish F-16 that was trying to engage a Syrian Air Force jet; when the Turkish aircraft fired missiles guided by an AWACS aircraft, the missiles missed their target.[558]

Syria has become a testing ground for Russian military equipment, including SIGINT and jamming aircraft. While the Tu-214R had previously seen action in the Ukraine conflict, both it and the IL-22PP are being heavily tested in Syrian operations as Russia increases its electronic warfare and ISR targeting capabilities. These capabilities support what Russia calls the "reconnaissance-strike complex," which feeds high-precision, long-range weapons with real-time intelligence data and accurate targeting information to increase the accuracy and throughput of airstrikes.[559] Combat situations, however, can be tragically unpredictable. An IL-20 was shot down over Syria in September 2018 by what was believed to be Syrian air defense forces. As the Syrian forces were shooting at Israeli aircraft that were striking a facility in Syria linked to Syria's chemical weapons program, the IL-20 mistakenly crossed the path of the Syrian air defense missiles and was destroyed.[560]

Outside Syria, Russian maritime reconnaissance and anti-submarine warfare (ASW) aircraft from Russia's Northern Fleet were reported in early 2020 to be flying much further south into the so-called Greenland-Iceland-UK (GIUK) gap than normal. The GIUK gap forms a chokepoint in the northern Atlantic that is critical for the Russian navy in case of a conflict, and Russian Tu-142 maritime reconnaissance and ASW planes conducted at least three flights into the gap in February and March 2020. The main mission of these planes is to identify NATO submarines and conduct ELINT collection.[561]

During the Cold War, the Soviet Union reportedly used non-military aircraft, such as Aeroflot airliners and airliners from other Warsaw Pact countries, to collect SIGINT as they overflew European countries and possibly the United States. The airliners would collect SIGINT from facilities along their flight path and would occasionally veer from their planned flight path to overfly specific facilities.[562] There has been no public reporting of this activity since the end of the Cold War, although the intensity of Russian intelligence collection operations and the resurrection of Cold War-era methods under the Putin presidency suggest the possibility that Russia could consider doing it again.

Satellite-Based ELINT

In the 1960s, the Soviet Union launched its first ELINT satellite under the Tselina program. The Tselina collectors were capable of geolocating and characterizing electronic emitters, such as radars and communications systems, particularly those used in anti-missile, anti-aircraft, and air force and navy electronic systems. This information can be used to target those emitters in case of war, especially to remove threats to Russian military forces, and to identify the specific characteristics of radars in order to develop radar countermeasures, such as jamming or blinding radars. This collection enables the development of an electronic order of battle, which allows Russia's military to develop countermeasures or to circumvent the foreign military's radars if necessary. Before Tselina, the Soviet Union had to use airborne platforms, like the IL-20, to collect information about U.S. air defense and missile defense radars, but these airborne platforms could not overfly U.S. territory and so could not see far into the U.S. mainland. The Soviet Union needed a system that could cover a broader range.

Initially, the Soviet Union launched two versions of the Tselina, a broad view satellite (Tselina-O) and a more detailed view collector (Tselina-D). The early versions did not have real-time data downlinks, and they stored data until a downlink could be established with a Soviet-based ground station. A later version, the Tselina-2, first launched during the 1980s, was capable of real-time data transmission via a series of relay satellites. In addition to collecting on radars, Tselina satellites were used as an alert system to observe the intensity of communications—if military communications became more frequent or concentrated, it could be an early warning indicator of pending military activity. Tselina was never a COMINT system, however, meaning it never collected voice communications—that was done and is probably still done by ground-based systems. Thus, the Tselina system was used almost exclusively for military purposes. Over 130 Tselina satellites were launched throughout the history of the program, and they were expected to operate for about six months. The last three Tselina-2 satellites were launched in 2000, 2004, and 2007, and the program was phased out.[563]

A complication of the Tselina system was that both the satellite and the launch vehicle that put it into space were manufactured in Ukraine. Additionally, the satellites were launched from the Baykonur launch complex in Kazakhstan. The dissolution of the Soviet Union slowed the program and forced Russia to recreate these capabilities internally. By the late 1990s, Russia was transitioning the system manufacturing and launching components to Russian territory. Tselina was eventually phased out in favor of a fully Russian program.[564]

In the 1960s, the Soviet Union launched another series of ELINT satellites called US-P (Russian acronym for Passive Guided Satellite), which was a passive ELINT satellite specifically focused on maritime targets. Soviet/Russian forces used US-P satellites to locate and target ships at sea, which a satellite, situated at the vantage point of hundreds of miles from the Earth, can do more effectively than another ship on the Earth's surface. Each US-P satellite remained in orbit for one to two years, and the last one was launched in 2010. Also part of that maritime program was an active radar satellite, called US-A (Active Guided Satellite, later known as RLS). The active radar made it possible to pinpoint large metal naval vessels at sea. An active radar needed high amounts of electrical power to send out an active radar pulse and receive the echoes, however, and the US-A active radar was powered by a small nuclear reactor to generate enough electricity. The US-A satellites lasted only three or four months before they ran out of fuel, and the last US-A satellite was launched in the late 1980s. Both the US-A and the US-P systems have been phased out.[565]

In 2009, Russia launched the first of four ELINT satellites, called Lotos-2, under the new Liana program. The program began in 1993, but numerous funding and technical issues delayed the first satellite's launch for 16 years. The first Lotos-2 satellite lasted about three years, and three additional satellites have since been added to the Lotos constellation—launched in 2014, 2017, and 2018—leaving three currently in orbit. Liana is more capable than the Tselina system, giving Russia increased visibility on electronic emitters, especially radars, which are a very important intelligence target given Russia's anxiety about theater missile defense. The Liana system consolidates and replaces the formerly separate collection of both land and maritime targets.[566]

Russia's ELINT satellites are run by the GRU Sixth Directorate, the same directorate that manages Unit 26165, which conducted intrusions into the German Bundestag in 2015 and the U.S. Democratic National Committee in 2016, as well as many other computer-based collection operations. All of the GRU's SIGINT capabilities, whether space-based, ground-based, sea-based, airborne, computer-based, or close access, are run from the Sixth Directorate.

SATELLITE-BASED GEOINT

Russia maintains a varied set of GEOINT and early warning satellites. These satellites provide photographic and radar imagery, infrared warning, and cartographic capabilities. For most of the Soviet era, the GRU ran the Zenit program, which consisted of small imagery satellites that stayed in orbit for an average of one to two weeks. Over 650 Zenit satellites were launched from 1962 to 1994. The Zenit program was eventually supplemented in the 1970s by the Yantar program, which had a better camera and could remain on station longer—over four weeks. The program continued to improve over time until it was replaced by the Persona series in the 2000s.

Beginning in 1981, the Yantar series also included a cartographic capability that allowed the Military Topographic Division of the General Staff to produce detailed maps of the Earth's surface, including elevation data developed from space. As a result, practically any area of the Earth's surface could be mapped, including countries that were out of reach of the Soviet military. Yantar cartographic satellites, later known as Kometa, were launched about one per year from 1981 to 1994.[567] The dissolution of the Soviet Union slowed the production of these satellites; between 1995 and 2005 only three more were launched. The last Yantar cartographic satellite was replaced by a new series, known as Bars-M1 and -M2, which was launched in 2015 and 2016.[568]

The Araks satellite (also called Arkon-1) reportedly carries panchromatic and near-infrared sensors with a one-meter resolution. Program development began in 1984 but experienced long development delays; the first satellite was launched in 1997 and the second in 2002. Only these two satellites were launched, each with a lifespan of about four years. According to a *RussianSpaceWeb* report, the system was highly successful, and the ground station could not keep up with all the high-quality imagery coming from the Araks-2.[569]

The current Russian imagery satellite series is the Persona system. Three Persona satellites were launched in 2008, 2013, and 2015, with a seven-year life expectancy. The program was conceived in the 1970s as a long-life satellite to replace the short-lived Yantar. Many program delays occurred and, even after initial launch in 2008, the first Persona satellite failed after less than a year. The satellite flies in a sun-synchronous orbit, meaning it moves around the Earth so it is always directed where the sun is shining. Consequently, it is capable of imaging virtually any point on Earth. Persona imagery was released publicly for the first time after the MH17 airliner shootdown, with the Russian government claiming the images proved that Ukraine was at fault.[570]

Russia also has a radar imaging satellite called the Kondor, first launched in 2013. The Kondor program took about ten years from initiation to launch, with technical difficulties and funding shortages slowing the system's delivery. Only one satellite has been launched so far.[571]

Additionally, the Soviet Union operated an infrared early warning satellite, originally called the US-K (Russian acronym for Continental Guided Satellite), to detect missile launches based on their heat signatures. The US-K program, also known as the Oko system, ran from 1981 until the last satellite in the series was launched in 2012.[572] As with other satellite programs, the US-K series slowed in the late 1990s and early 2000s, but was eventually replaced by the *Единая космическая система* (Unified Space System; EKS Kupol) series, three of which were launched from 2015 to 2019. This satellite capability continues to operate in conjunction with ground-based anti-aircraft radar systems that monitor the air approaches to Russia[573] and is important for Russian intelligence because it would give warning of a U.S. missile attack.

Russian space-based technical collection programs are focused almost entirely on military missions. While ground-based collection systems are used for various missions, including political, economic, and military collection, the GRU's satellite programs are focused on locating and monitoring military movements, characterizing radar and communications systems, and missile early warning.

COMPUTER-BASED COLLECTION

Previous chapters have discussed the use of computer intrusions (often called cyber activities) in multiple Russian intelligence missions, including political and military intelligence collection and covert operations. Russian computer intrusion operations follow a typical pattern employed by what are called advanced persistent threats (APTs), sophisticated network intrusion teams that can maintain their presence unnoticed for extended periods, waiting for the right moment to act or the right information to collect.

The typical pattern for intruding into a system has several steps. The specific tactics used in each step differ by each APT, just as one burglar uses a different type of lock-picking method than another. Computer security companies have identified specific intrusion teams based on the specific tools and methods they use.

An APT follows a general pattern of activity when identifying and penetrating a target system. The steps include:

- **Reconnaissance/research:** An APT team studies a targeted entity in depth and finds the weak links in the network before attempting to penetrate it. The weak links might come from an organization not keeping patches up to date, from network users who are not sufficiently trained to identify suspicious emails, or from thumb drives that are used to move information from one computer to another. The research phase identifies those vulnerabilities.
- **Preparation:** An APT team might develop and test tools and techniques specific to the targeted network. This may require writing or acquiring new code to elude a specific security system.
- **Incursion:** The APT team finds a point of entry into the targeted network. The entry point might be facilitated by a phishing email

containing malware that embeds a back door into the system as soon as someone clicks on it. Entry might also involve a password capturing system that records passwords for later use, or when an APT team uses newly developed software to take advantage of the specific system's vulnerabilities. Additionally, entry might involve exploiting what is called a "zero-day" vulnerability, which is a flaw in the system software that a manufacturer has not previously identified. An APT will hide the tracks toward that entry point by penetrating a string of compromised third-party computer systems, called hop-points, along the path, making it look like the intrusion is coming from somewhere else.

- **Establish presence:** The software that the APT team installs will "call home" to a command-and-control server when it is inserted into the target computer system, reporting where it is in the system architecture and opening the path for further instructions.
- **Discovery:** Once safely in the system, the APT team searches for data and assets of value, exploiting insider accesses to a targeted computer system either to collect data directly or as a stepping-stone toward other accesses within the system.
- **Capture:** The APT team will remotely move through the network collecting information. Usually, the ultimate goal of an intrusion is to collect intelligence, and, once on the inside, a hacker can find the desired information.
- **Exfiltration:** To take advantage of the collected information, the APT team needs to find a way to communicate it out of the targeted network to headquarters. Exfiltration is the hardest part of an operation, because it involves moving sometimes large amounts of data out of the system, which can be seen by system administrators.

What the Russian government does with the exfiltrated information may vary, from applying it to other intelligence operations, such as using it to identify potential HUMINT targets; using it for political or economic decisionmaking; leaking it to facilitate a disinformation operation; or using it to sabotage the system itself. In Russia, the information is usually passed from a collection organization to another element within the intelligence or security service to execute the operation.[574]

Russian computer-based intelligence activity has become much more prevalent since around 2008, and it has especially increased in use to fulfill internal security and political collection requirements. Although the United States is prominent in Russia's targeting, Russian intelligence activities have shown a wide diversity of interests and target countries over the past decade. Any country that is developing policy toward Russia is of interest to Russian intelligence, especially if that policy involves NATO. Attribution of computer-based collection is always difficult. But, as noted in previous chapters, numerous reported Russian-sponsored computer intrusion events since 2014 show that Russian computer-based operations are not always as stealthy as they are professed to be. Computer security companies have successfully attributed dozens of incidents directly to Russia's intelligence services—mostly the FSB and GRU, and more recently, with the SolarWinds operation, the SVR. Some attacks have successfully penetrated the targeted entity, while others have been caught and thwarted, and then publicly announced so that other potential targets could close vulnerabilities.

CONCLUSION: TECHNICAL COLLECTION IN COOPERATION WITH HUMAN PLATFORMS

Two general themes emerge from Russian technical collection systems and provide insights into the threat they pose and the challenges they face. The first theme relates to the impact that the dissolution of the Soviet Union has had on technical systems. After the Russian Federation became an independent country separate from the 14 other former Soviet republics, Russian technical collection programs experienced a series of setbacks. The first was that Russia's economy suffered greatly, making high-cost programs like satellite reconnaissance systems difficult to afford. Consequently, research and fielding of technical collection systems were significantly delayed throughout the 1990s. However, Russia's economic growth in the 2000s, fueled by oil sales, pushed these long-delayed systems to completion. Modernized versions of satellite-based collection platforms began to appear around the 2010 timeframe, and several of the systems have begun operation since 2015.

Russia's economic downturn was also accompanied by a brain drain, which limited the number of highly trained specialists needed to conduct research and manufacture highly technical intelligence collection systems. According to research done by the Russian Presidential Academy of National Economy and Public Administration in 2018, an increasing number of educated Russians are leaving the country for economic and political reasons.[575] The Russian government is attempting to combat this trend through patriotic messaging to its people.

The dissolution of the Soviet Union also deprived Russia of manufacturing and launch sites for satellite-based systems and foreign sites for ground-based systems that had previously been integrated into the Soviet-era intelligence system. These included rocket engine and electronics manufacturers in Ukraine and a launch site in Kazakhstan, along with collection sites in Soviet-allied countries around the world. These changes have forced Russia to either negotiate agreements with new allies or relocate capabilities to Russian soil. For example, although Russia still has access to the Baykonur launch complex in Kazakhstan from which it has traditionally launched its reconnaissance satellites, that site is now located in a foreign country. Since 2005 Russia has pursued a launch site in the Russian Far East to "confirm Russia's leading technological status;" the Vostochniy Launch Site in Russia's Amur Region launched its first unmanned vehicle in 2015 and its first manned vehicle in 2018.[576] The situation in Ukraine is more complicated, especially since Russia illegally annexed Crimea in 2014 and Ukraine cut off commercial ties with Russia's space development ventures. Russia has been forced to replace Ukraine-based manufacturing capabilities.

The second theme relates to the integration of technical and human collection capabilities. While Russian computer-based operations have increased in quantity and aggressiveness in the past decade, Russian intelligence incidents that have been revealed publicly show a continued mix of HUMINT, close access technical operations, open-source intelligence, satellite-based collection, air- and sea-based collection, and computer intrusions. No tool is off the table, and the various platforms at Russia's disposal are often used in concert with each other. For example, code clerks are recruited as human sources who can provide information to support SIGINT collection. SIGINT systems monitor local counterintelligence surveillance communications to support HUMINT operations. HUMINT tradecraft is used to deploy close access SIGINT collectors, and human sources are dispatched abroad to collect information to use in computer-based covert operations. The systems are often mutually supportive.

CHAPTER 10

THE FUTURE OF RUSSIAN INTELLIGENCE

In a monograph titled *Putin's Hydra*, Russian state security expert Mark Galeotti has presented a range of options for how a country's intelligence and security services manage their operations: either well or poorly, and in a manner that is either aggressive and offensive or passive and defensive (see Figure 27).[577] While there is little question that Russia's services are aggressive, the evidence is less clear that they are well managed. An aggressive and well-managed service would be a formidable instrument of statecraft, and Russia's aggressive covert operations in Ukraine have shown themselves to be tools for Russia to achieve its strategic objectives. However, an aggressive and poorly managed service would be a detriment to Russia and could even be counterproductive. At times, Russian actions have appeared to exhibit bad tradecraft and operational security that have revealed Russia's involvement in operations that the government probably intended to remain clandestine or covert.

Galeotti points out that Russian services have performed well at the tactical level against targets within easy reach, especially in Ukraine. At the strategic level, however, Russian intelligence services either did not inform the Russian leadership about the intensity of the Western reaction that Russia's covert operations in Ukraine or Western Europe could face, or Russian leaders did not pay attention to these intelligence assessments.[578] Russian intelligence collection and covert operations have been revealed publicly time after time since 2010, including foreign arrests of illegals, Russian arrests of officers for fraud and robbery, the attribution of dozens of Russian computer-based operations, the exposure of an unmistakably Russian hand behind assassinations and government manipulation, the arrests and expulsions of large numbers of officers under diplomatic cover, and continuing defections from the ranks of Russian services.

Figure 27. Management of Security Services

	Well Managed	Poorly Managed
Aggressive	Formidable instrument of statecraft	Dangerously counterproductive
Defensive	Strong shield against enemies	Do little harm in times of peace but no protection in hostile conditions

Source: Figure created by author from array of management approaches described in Mark Galeotti, Putin's Hydra: Inside Russia's Intelligence Services *(London: European Council on Foreign Relations, 2016), 14-15,* https://ecfr.eu/archive/page/-/ECFR_169_- _PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf.

With that mix of well-managed and poorly managed forces, what will drive Russian intelligence in the future? Russian services face both advantages and challenges. Advantages include Russia's ability to portray its intelligence services as invulnerable and heroic. However, the challenges are significant; some of which have been with Russia for a long time, while others result from technological and demographic changes.

We can assess the threat of Russian intelligence by applying the threat equation—threat=intent x capability x opportunity—and looking at how each factor might change over time. Intent is an agency's will to perform an act; it is based on the policies and strategies of the government that stands behind the agency, as well as the mindset of the officers in the agency. Capability is the agency's physical means to perform an act, including its manpower and technology assets. Opportunity is the spatial-temporal relationship between the agency's assets and the targets, including the reach and accesses that the agency enjoys.[579] This final chapter will apply these factors to Russian intelligence and state security services and to the threat that Russian services pose.

THREAT EQUATION: INTENT

Russian intent is informed by its threat perceptions, which drive actions, and by its perceptions of success, which remove inhibitions and create a sense of invulnerability. In Russia's threat perception, the country is under siege by a Western system that is trying to prevent Russia from regaining its rightful place in the world. In that perception, the United States is a destabilizing factor in the world. When Russian leaders discuss intelligence and covert activities, they invariably do so in terms of a threat to Russia, unless they are heroizing a past officer or exploit. As Russia articulates threats to its national security, it employs its national security tools—like intelligence and state security services—to mitigate those threats. Russia views itself as being at political war, as opposed to military war, with the West, especially with the United States. Thus, it uses its intelligence, counterintelligence, and covert action capabilities to their full extent to fight that political war.

Russia's relationship of distrust with the West is not likely to change soon. Some U.S. commentators assert that Russia has had preferred candidates for President of the United States and has manipulated the U.S. public to ensure the victory of its preferred candidate. Although Russia may dislike one candidate more than it dislikes another, it is unlikely that any Russian leader trusts any U.S. president. Putin has seen a steady stream of U.S. presidents who began their presidency saying positive words about Russia but subsequently made decisions contrary to Russian interests.

In the 1990s, U.S. President Bill Clinton developed a close personal relationship with Russian President Boris Yeltsin, and the leaders claimed to be able to pick up the phone and discuss issues at any time. President Clinton, however, supported NATO enlargement into former Warsaw Pact countries and authorized the bombing of Russia's ally Yugoslavia, directly against Russia's vocal opposition. In the early 2000s, when the United States faced a severe terrorist threat, new Russian President Vladimir Putin was the first world leader to express condolences and support for the United States. Several months before that, U.S. President George W. Bush said, "I looked the man in the eye. I found him very straightforward and trustworthy—I was able to get a sense of his soul."[580] Then, President Bush authorized the deployment of theater missile defense systems, supported the membership processes for Baltic republics to join NATO, and oversaw a U.S. Government that openly criticized Russia's brutal methods in Chechnya. When "color revolutions" occurred in the former Soviet republics of Georgia, Ukraine, and Kyrgyzstan during the Bush Administration, Russian suspicions that the United States was trying to encircle Russia with anti-Russian regimes grew.

Later in the decade, President Barack Obama said positive things about Putin during their first meeting and initiated a "reset," promising to improve relations that had frayed under the previous U.S. President. A few years later, President Obama authorized NATO military action in Libya that forcibly and humiliatingly removed Moammar Qadhafi from power. Secretary of State Hillary Clinton, who had initiated the reset with Russia, spoke positively about Russian protesters who were demonstrating against Putin's return to the presidency in 2012—and later became a candidate for the U.S. presidency. President Obama also authorized sanctions against Russia for annexing Crimea. He expelled 35 Russian officers from the United States in retaliation for meddling in the 2016 U.S. presidential election, after the U.S. Intelligence Community issued a rare public analysis of Russian government interference in the U.S. election. Finally, President Donald Trump promised to improve relations with Russia, claiming to be able to work well with Putin. President Trump subsequently increased sanctions on Russia, ordered a Russian consulate and recreational facilities to be closed, and then expelled 60 more Russians after the assassination attempt on Sergey Skripal in the United Kingdom. Former Russian Prime Minister Dmitriy Medvedev called the Trump Administration a "period of disappointment."[581]

Putin has learned from these experiences. He has no illusions that any U.S. president will support Russia or benefit Russian interests. Putin will authorize clandestine collection operations and covert action to protect Russia from what he views as an American-led Western political assault on Russia, led by a series of U.S. presidents who, in the Russian leader's view, have betrayed Russia.

Russian intent is also informed by its perceptions of its own successes, which embolden Russia and increase the likelihood that it will use its intelligence and covert operations capabilities. Russia benefits when it can portray its intelligence and covert operations as victorious, and it further benefits when its adversaries perceive Russian operations in the same light. One of the most significant successes of Russian intelligence is that it has manufactured a mythos of an unstoppable, irreversible force that is futile to fight—a mythos that serves Vladimir Putin well. As part of this mythos, Russian intelligence leaders claim that Russian illegals are envied by Western intelligence services. As long as Russia can maintain that mythos, both with its own people and abroad, its intelligence services will continue to have success.

Russian leaders have heroized their intelligence officers to the point that many in Russia now see them as a force for good—a significant change from the early post-Soviet era. In January 2020, the SVR director declassified the identities of seven retired KGB/SVR illegals, several of whom had operated against the United States. In each case, the announcement claimed that the named former illegal had done exceptional work in collecting highly sensitive information in support of Russia's interests.[582] Since 2012, the Russian government has minted postage stamps honoring 18 MVD officers, 11 FSB officers, 5 military intelligence and special operations officers, 2 military counterintelligence officers, and a former SVR director, along with commemorative stamps for Soviet-era illegals, and the founding of the SVR, GRU, FSB, Border Guards, and SIGINT collection.[583] The Russian government has also awarded numerous FSB and GRU officers the title Hero of the Russian Federation during that time. These types of announcements are intended to make the Russian population proud of their intelligence officers, while also giving the Russian government an opportunity to portray itself as invariably successful.[584]

The life of a state security worker is popular among some Russians for a variety of reasons: reputedly being a good paying job with solid job security and offering the feeling of being in a position of power. Government propaganda unceasingly trumpets patriotic messaging that portrays state security officers as honorable, the cream of society, self-sacrificing, and thinking only of interests of the state. On the other hand, these efforts may occasionally fall short due to Russians' perceptions of corruption within the state security services, a continuing fear of state security, and disagreements with agencies' methods, like assassinations and Internet monitoring,

Polls inside Russia are mixed regarding the popularity of Russia's intelligence services and the success of these public relations efforts. A 2018 survey found that 45 percent of parents and grandparents wanted their children to work for security services, reportedly up from 29 percent in 2001. The survey also claimed that 50 percent of young Russians (up to 30 years old) wanted to work for security services.[585] However, a different survey in October 2019 claimed that only 20 percent of parents or grandparents would welcome their children or grandchildren joining an intelligence organization.[586]

Despite the positive image that the Russian government portrays of the life of security service workers, those workers' lives are far from glamorous. Although security service workers enjoy some privileges, such as long vacations and free passes for public transport, in the words of one Russian journalist, "The FSB, GRU, FSO and the SVR… are not gods." Security service workers' travel is restricted: they can only take vacations within the borders of the Russian Federation and cannot leave the country for ten years after they leave the service. Their salaries are not high—35,000 to 80,000 rubles ($400-1,000) per month—making it difficult for some officers to meet economic needs. Rank-and-file workers live in normal, rundown Russian housing, while senior leaders enjoy huge riches. With reportedly little comradeship, mistrust is rife among staff. Post-traumatic stress is a reality for security staff personnel who have served in special operations units, with little psychological support offered.[587]

Targets of Russian operations need to be careful not to exaggerate the success of Russian operations, thereby feeding into Russian intelligence services' own narrative of being all-powerful and unstoppable. Disinformation operations have created room for Russian maneuvering of external perceptions; for example, Russia has gained a reputation for causing discord and deepening divides in its adversaries' political systems. Thomas Rid, in his 2020 book *Active Measures,* assesses to the contrary that Russia's election manipulation activities in the United States have not been particularly successful, despite the media attention they have received. Reports often use social media "impressions" as a measure of Russian success; however, "impressions" may grossly exaggerate real impact. As Rid concludes: "Online metrics, in short, created a powerful illusion, an appealing image—the metrics created an opportunity for more, and more convincing, disinformation about disinformation. Willfully exaggerating the effects of disinformation means exaggerating the impact of disinformation."[588] The resulting effect could make Russia's narrative a self-fulfilling prophecy.

Russian intelligence and security services' track record is far from perfect, despite their positive self-portrayal. Russian intelligence and covert activities have experienced some successes but also many failures. Covert operations have been regularly revealed publicly, including disinformation operations (e.g., those that followed the athlete doping scandal, MH17 shootdown, U.S. election interference, Skripal attack), foreign government manipulation (e.g., United States, France, United Kingdom, Spain, Montenegro, North Macedonia), undeclared military operations (e.g., Ukraine, Libya, Central African Republic, Mozambique), and attempted and successful assassinations (Navalny and Skripal among the former and multiple Chechen militants in the latter). Russia has experienced a number of intelligence setbacks, such as diplomatically covered officers expelled in large numbers; illegals operations compromised in multiple countries (e.g., Canada, United States, Germany, Spain), reportedly leading some Russians to question the value of illegals;[589] and computer-based collection and sabotage operations regularly attributed to Russia publicly, despite Russian intelligence services' attempts to conceal their involvement. These revelations damage Russia's credibility in the world.

The perception of Russia among Americans and Europeans is at its lowest since the dissolution of the Soviet Union, to a large extent due to Russia's own aggressive intelligence and covert operations. The downward trend began about the time that Edward Snowden appeared in Moscow and was granted political asylum. Subsequent events, like the Russian annexation of Crimea, revelations of election meddling, and the Skripal assassination attempt, have pushed Russia's reputation among Americans further down.[590] Since 2015, Russia has been perceived as first or second on the list of the United States' greatest enemies, according to a Gallup poll. Russia has either led the pack or trailed behind only North Korea since 2015.[591] A similarly negative trend has occurred across Europe.[592]

This downturn damages Russia's ability to conduct intelligence operations, making it harder for Russian officers to find people willing to cooperate and develop relationships. Because many Americans and Europeans suspect the veracity of any messages coming from Russia, Russian disinformation messages may resonate less with them. Western targets need to keep a balanced perspective about Russian intelligence activities. While Russia's operations should not be underestimated, they should also not be exaggerated, because expanding them beyond reality plays into Russia's narrative of an unstoppable intelligence force.

THREAT EQUATION: CAPABILITY

Capability is a mix of manpower and technology. Russia has experienced some disadvantages in the area of manpower, while technology has been both a blessing and a curse.

Russia's overall demographic decline is trending toward fewer young people being trained in technological fields, and some of those are choosing to emigrate due to a lack of both economic and political opportunities, leaving fewer young people to take the new positions. In addition, the FSB has experienced several waves of disparaging news that make FSB officers look like corrupt egotists. In 2015, for example, a group of graduates of the FSB academy paraded through the streets of Moscow in dozens of expensive Mercedes SUVs, honking their horns, cheering, and posing for a group photo. A video of this behavior elicited a highly negative reaction from the public and from Russian officers, who considered it a gross violation of professionalism.[593] The stunt—a possible indicator of the caliber of available recruits—did not sit well with the FSB leadership. The FSB announced a few weeks later: "Principled personnel decisions have been taken toward the guilty individuals, changing the condition of their service. Severe disciplinary measures against the leadership of the Academy, including the demotion of several leaders [and] their firing, will be taken."[594]

The FSB has also been the target of several high-profile corruption investigations in the past several years, further tarnishing the agency's public image and damaging the FSB's ability to perform its mission. An officer in an FSB counter-corruption unit was arrested in May 2019 with $185 million cash in his apartment. His arrest was probably the result of infighting within the FSB, but it painted a picture of the FSB as part of the corruption problem rather than the solution.[595] In July 2019, seven FSB officers were arrested for armed robbery, possibly targeting corrupt government officials; the FSB officers had reportedly been tipped off that a corrupt official was planning to deposit a large amount of cash, and they robbed him as he entered the bank.[596]

Demographic factors also impede Russia's ability to find appropriately skilled individuals for specialized roles in its intelligence and security services. Russia struggles to identify reliable, loyal people to work as illegals abroad, and the heroizing of its illegals program is at least in part designed to attract the most patriotic and motivated people to become illegals. Individuals with special skills are also needed to drive improvements in remote sensing technology and satellites. Russia has encountered difficulties in training enough people in the highly technical fields that support satellite-based intelligence operations.

Technology itself is another part of the capability factor. In some ways, technological improvements have increased Russian intelligence and counterintelligence capabilities. Biometrics technology facilitates counterintelligence and internal security operations. Increased installation of cameras in public places, accompanied by facial recognition technology, improves Russian counterintelligence capabilities. The Russian government has used the

COVID-19 pandemic to increase the monitoring of its own people using a variety of tracking technologies. Russia is also implementing improvements in Internet and communications tracking. Technology can also support intelligence and covert operations by allowing remote access to some computer systems and making bulk exfiltration of data more possible.

Modern technology, however, can also make intelligence operations less capable. Biometrics technology, originally invented to inhibit terrorist travel, makes Russian clandestine operations more challenging when the technology is applied abroad. Sharing databases across borders enables the identification of false travelers, making it more difficult to travel clandestinely. As former CIA officer Robert Grenier and others have noted, clandestine operations cannot be conducted today as they used to be.[597] Russia has probably responded to this challenge by changing who it selects to be illegals, selecting some people who operate openly as Russians, albeit without overt connections to the Russian government.

THREAT EQUATION: OPPORTUNITY

Several factors increase the opportunities and reach of Russian intelligence and covert activities. However, the factors that provide Russia with greater opportunities each have corresponding measures that can reduce those opportunities.

Russia's placement of officers in various types of covers—diplomatic, nonofficial, and illegal—offers opportunities for Russia to access a variety of people and data. Each has advantages that allow Russian intelligence services to operate in different social circles, opening the possibility for placement and access to a wide spectrum of information. The very purpose for those options is that each offers different advantages for access. However, mass expulsions and public arrests of Russian intelligence officers at least temporarily reduce opportunities to engage with sources or to operate embassy-based SIGINT collection platforms. When the United States closed the Russian consulate in San Francisco and Russian diplomatic resorts in Maryland and New York in 2016, the threat equation element of opportunity was reduced; the facility closures both reduced the number of officers in the country and removed accesses to electronic signals that Russian services cannot otherwise reach. Additionally, the United States pulled out of the Open Skies Treaty in 2020 presumably, at least in part, to reduce Russian collection opportunities.

Global computer connectivity also provides opportunities for Russian intelligence activities, although those opportunities can be thwarted. Russia can use the accessibility that computer networks provide to collect intelligence in some places where it cannot easily or securely send collectors in person. However, as intrusions are discovered, defensive efforts, like patches and threat awareness, reduce Russian collection opportunities and make remote intrusions more difficult. Additionally, not all information can be accessed remotely via the Internet, and sometimes a human insider is required to provide access to internal data. At other times Russia needs to dispatch close access SIGINT collectors and computer intrusion specialists to gain access to signals that cannot be reached remotely, which is riskier. Efforts to reduce Russian collection opportunities can force Russia to use riskier and more expensive measures.

Combining and collaborating across intelligence disciplines offer increased opportunities to access sources that might otherwise be inaccessible. As Russian intelligence services use one intelligence discipline to tip and cue another, they extend the reach of the intelligence system overall. This collaboration might include, for example, tasking a HUMINT source to gather information that facilitates SIGINT or computer-based operations, or collecting signals that warn of counterintelligence operations targeting HUMINT operations. Russian intelligence services are notorious, however, for interagency battles and rivalries. Clashes between intelligence and counterintelligence organizations, or between civilian and military intelligence organizations, reduce both capabilities and opportunities.

At a more strategic level, anti-U.S. sentiment around the world creates opportunities for Russian intelligence. As long as there are populations in the world that oppose the United States, whether politically, militarily, or economically, Russian intelligence and covert information operations will have fertile ground in which to operate. People who already are willing to act against U.S. and Western interests are easier to persuade to cooperate with Russian intelligence operations than those who favor the West. The Soviet Union and Russia have relied on anti-U.S. sentiments for intelligence activities since the Cold War. Counteracting that Russian opportunity extends far beyond the intelligence or counterintelligence realm, requiring the United States and the West to develop effective international relations and to increase positive views of democratic ideals around the world.

Finally, an open, democratic society offers opportunities for exploitation by an aggressive Russia—covert disinformation operations are hard to stop in an open society. Christopher Walker of the National Endowment for Democracy describes the advantage that Russia potentially enjoys in the information realm, defining Russia's use of what he calls "sharp power" as:

> An approach to international affairs that typically involves efforts at censorship or the use of manipulation to sap the integrity of independent institutions. This approach takes advantage of the asymmetry between free and unfree systems, allowing authoritarian regimes both to limit free expression and to distort political environments in democracies while simultaneously shielding their own domestic public spaces from democratic appeals coming from abroad.[598]

Using these methods simultaneously, Russia can protect itself from foreign infiltration, as envisioned in the mythical Dulles Plan, by taking advantage of the freedom of expression afforded by democratic systems. Russia's approach has changed little since the Cold War, when Soviet services routinely disseminated falsified information and counterfeit documents and cast Western society in a negative light to prevent the Soviet population from viewing it as attractive. However, the opportunity that open societies provide for access is also the very characteristic that strengthens them. It would be to the West's detriment to diminish its openness just to reduce Russian or other countries' intelligence or covert operations opportunities. A democratic society needs to recognize and play to its strengths, allowing freedom of all positions to be voiced, including positions that highlight injustices elsewhere, not just in its own society.

FINAL ANALYSIS

While it would be wrong to dismiss Russian intelligence as a threat, it would also be wrong to view Russian intelligence as "10 feet tall and bullet proof." Russian intelligence and state security services look in many ways like they did during the Andropov era: still run by leaders raised in the chekist mindset, who view the West as an eternal and unchanging threat and who connect that external threat to manifestations of popular dissatisfaction inside Russia. That dynamic sets the foundation for the "intent" factor of the threat equation. Russia retains highly proficient collection and covert action capabilities, both human and technical. Russian intelligence platforms are located worldwide, inside computer networks, and in space, giving Russia global intelligence reach and opportunities. Nevertheless, Russian intelligence has weaknesses that can be exploited. Probably among the worst of those weaknesses is its own hubris—a sense that it is invulnerable. If Russia can portray its successes as being the result of a well-managed, powerful, patriotic system, and simplistically explain away its failures as nothing but "Russophobia," it can weather failures and capitalize on successes. Similarly, if the victims of Russian intelligence activities and covert activities focus only on Russia's strengths and ignore its weaknesses, the victim itself grants those activities greater potency and effectiveness. However, publicly revealing Russian operations as aggressive, antagonistic, and in some cases inept can diminish Russia's self-manufactured lustrous intelligence reputation.

The purpose of this book is to provide the analytic tools with which to assess that threat in a balanced way, to break the threat down to its component parts of who, why, and how, and to view each component within its own context, along with its strengths and weaknesses. Russian intelligence is a formidable adversary, but it is not invulnerable. Targets of Russian intelligence activities need experts who see those activities in a balanced way. This book is designed to begin the process of building that expertise.

ABOUT THE AUTHOR

Kevin Riehle is an associate professor at the University of Mississippi, Center for Intelligence and Security Studies. He spent over 30 years in the U.S. Government as a counterintelligence analyst studying foreign intelligence services, finishing his government career as an associate professor of strategic intelligence at the National Intelligence University. He received a Ph.D. in war studies from King's College London, an MS of strategic intelligence from the Joint Military Intelligence College, and a BA in Russian and political science from Brigham Young University. Dr. Riehle has written on a variety of intelligence and counterintelligence topics, focusing on the history of Soviet and Eastern Bloc intelligence services. In 2020, he published *Soviet Defectors: Revelations of Renegade Intelligence Officers, 1924-1954*. His articles have appeared in *Intelligence and National Security*, *International Journal of Intelligence and CounterIntelligence*, *Cold War History*, *Journal of Intelligence History*, and he has been interviewed by the International Spy Museum for its *Spycast* podcast series.

BIBLIOGRAPHY

Books, Monographs, Scholarly Articles, and Government Publications

ABN Universal Company website, http://www.abnuniversal.ru/content/page/company.htm.

Agabekov, Georgiy. *OGPU: The Russian Secret Terror.* Translated by Henry W. Bunn. New York: Brentano's, 1931.

Agabekov, Georgiy. *Секретный Террор* [*Secret Terror*]. Moscow: Terra, 1998.

Agabekov, Georgiy. *ЧК за работой* [*The Cheka at Work*]. Berlin: Strela, 1931.

Akhmedov, Ismail. *In and Out of Stalin's GRU: A Tatar's Escape from Red Army Intelligence.* Frederick, MD: University Publications of America, 1984.

Andrew, Christopher. *Defence of the Realm: The Authorized History of MI5.* London: Allen Lane, 2009.

Andrew, Christopher, and Oleg Gordievsky. *Comrade Kryuchkov's Instructions: Top Secret Files on KGB Foreign Operations, 1975-1985.* Stanford, CA: Stanford University Press, 1993.

Andrew, Christopher, and Oleg Gordievsky. *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev.* New York: Harper-Collins Publishers, 1990.

Andrew, Christopher, and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB.* New York: Basic Books, 1999.

Andrew, Christopher, and Vasili Mitrokhin. *The World Was Going Our Way: The KGB and the Battle for the Third World.* New York: Basic Books, 2005.

Australian Security Intelligence Organisation. "Moscow Instructions to Canberra." January 2, 1952. National Archives of Australia, A6283, folder 1, item number 4104669.

Australian Security Intelligence Organisation. "Statement by Petrova." October 14, 1954. National Archives of Australia. A6283, folder 15, item number 4104676.

Australian Security Intelligence Organisation Investigative Memo. April 13, 1953. National Archives of Australia, A6117, folder 8, item number 12077929, serial 154.

Australian Security Intelligence Organisation Memo. April 14, 1954. National Archives of Australia, A6283, folder 1, item number 4104669.

Australian Security Intelligence Organisation Memo. May 12, 1954. National Archives of Australia, A6283, folder 1, item number 4104669; duplicate in National Archives of Australia, A6283, folder 14, item number 4104675.

Australian Security Intelligence Organisation Report. "The Committee of Information ('KI'), 1947–1951." November 17, 1954. National Archives of Australia, A6283, folder 16, item number4104677.

Bagley, Tennant. *Spymaster: Startling Cold War Revelations of a Soviet KGB Chief.* New York: Skyhorse Publishing, 2013.

Ball, Desmond, *Soviet Signals Intelligence (SIGINT).* Canberra: Australian National University, 1989.

Barmine, Alexander. *Memoirs of a Soviet Diplomat.* London: Lovat Dickson, 1938.

Barmine, Alexander. *One Who Survived: The Life Story of a Russian Under the Soviets.* New York: G. P. Putnam's Sons, 1945.

Berman, Ilan, and J. Michael Waller, eds. *Dismantling Tyranny: Transitioning Beyond Totalitarian Regimes.* Lanham, MD: Rowman and Littlefield, 2006.

Boghardt, Thomas. "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign." *Studies in Intelligence* 53, no. 4 (December 2009): 1-24.

Booz Allen Hamilton, *Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations.* McLean, VA: Booz Allen Hamilton, 2020.

Brazhnev, Aleksandr, *Школа Опричников* (*Oprichniki School*) Kiev: Diokor, 2004.

British Embassy in New York to Foreign Office Telegram dated September 10, 1945. The National Archives, Kew, London, KV 2/1419, serial 3a.

British Embassy Washington Memo. September 13, 1940. The National Archives, FO 371/24845.

British Home Office Warrant. July 25,1930. The National Archives, Kew, London, KV 3/2398, serial 12a.

Bronnikov, Andrey, and Yelena Vavilova, *Женщина, которая умеет хранить тайны* [*The Woman Who Knows How to Keep Secrets*]. Moscow, Eksmo, 2019.

Bundesamt für Verfassungsshutz. "Hinweis auf aktuelle Angriffskampagne" ["Report on current attack campaign"]. Cyber-Brief Nr. 01/2016, March 3, 2016. https://www.verfassungsschutz.de/embed/broschuere-2016-03-bfv-cyber-brief-2016-01.pdf.

Bundesamt für Verfassungsshutz. "Hinweis auf aktuelle Angriffskampagne" ["Report on current attack campaign"]. Cyber-Brief Nr. 01/2018, June 7, 2018. https://www.verfassungsschutz.de/embed/broschuere-2018-06-bfv-cyber-brief-2018-01-neu.pdf.

Burtsev, Vladimir. "Police Provocation in Russia." *The Slavonic Review* 6, no. 17 (December 1927): 247-67. https://www.jstor.org/stable/4202167?seq=1.

Bush, George W. "User Clip: Bush Saw Putin's Soul." *CSPAN.* June 16, 2001, https://www.c-span.org/video/?c4718091/user-clip-bush-putins-soul.

Canadian Broadcasting Corporation. "The KGB Connections: An Investigation in Soviet Operations in North America." Documentary. 1982. https://www.youtube.com/watch?v=diT9oQjb8Ik.

Central Intelligence Agency. "The Examination of the Bona Fides of a KGB Defector." February 1968. U.S. National Archives and Records Administration, JFK Assassination Archives, document number 104-10150-10136.

Central Intelligence Agency. "Soviet-Sponsored Societies of Friendship and Cultural Relations." October 1957 CIA FOIA Reading Room.

Chebrikov, Viktor Mikhailovich, ed. *История Советских Органов Государственной Безопасности: Учебник* [*The History of Soviet State Security Agencies: A Textbook*]. Moscow: Dzerzhinskiy Higher Red Banner School of the Committee of State Security, 1977.

Cherkashin, Victor. *Spy Handler: Memoir of a KGB Officer. The True Story of The Man Who Recruited Robert Hanssen & Aldrich Ames.* New York: Basic Books, 2004.

Committee for State Security. "The KGB's 1967 Annual Report." May 6, 1968, Center for Preservation of Contemporary Documentation (TsKhSD), f. 89, op. 5, d. 3, ll. 1-14. Translated by Vladislav Zubok for the Wilson Center Cold War Intelligence History Project, History and Public Policy Program Digital Archive, http://digitalarchive.wilsoncenter.org/document/110403.

Corera, Gordon. *Russians Among Us: Sleeper Cells, Ghost Stories, and the Hunt for Putin's Spies.* New York: William Morrow, 2020.

Costello, John, and Oleg Tsarev. *Deadly Illusions: The KGB Orlov Dossier Reveals Stalin's Master Spy.* New York: Crown Publishers, 1993.

Council on Foreign Relations. *Cyber Operations Tracker.* https://www.cfr.org/interactive/cyber-operations.

CrowdStrike. *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed.* Sunnyvale, CA: CrowdStrike, 2020.

Cummings, Richard. *Cold War Radio: A Dangerous History of American Broadcasting in Europe, 1950-1989.* Jefferson, NC: MacFarland & Company, 2009.

Cybersecurity and Infrastructure Security Agency. "Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors." Originally published October 20, 2017, updated March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA17-293A.

Cybersecurity and Infrastructure Security Agency. "ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure." February 25, 2016. https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.

Dallin, David J. *Soviet Espionage.* New Haven: Yale University Press, 1955.

"Defection of KGB Officer." September 16, 1971. British government document contained in FBI file number 105-216642, serial 7, received by FOIA.

Defense Security and Counterintelligence Agency. *Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry.* Washington, DC: DSCA, 2019.

de Keghel, Isabelle. “Seventeen Moments of Spring, a Soviet James Bond Series? Official Discourse, Folklore, and Cold War Culture in Late Socialism,” *Euxeinos* 8, no. 25-26 (2018): 82-93.

Deryabin, Peter, and Frank Gibney. *The Secret World.* New York: Doubleday, 1959.

Dolmatov, Vladimir, ed. *Служба Внешней Разведки Российской Федерации 100 Лет: Документы и Свидетельства* [*The Foreign Intelligence Service of the Russian Federation at 100 Years: Documents and Testimonies*]. Moscow: Komsomolskaya Pravda, 2020.

Drozdov, Yuriy. *Записки начальника нелегальной разведки* [*Notes of a Chief of Illegal Intelligence*]. Moscow: Russian Biographical Institute, 1999.

Drugov, Fedor Pavlovich. “С Дзержинским в ВЧК: Исповедь раскаявшегося чекиста” [“With Dzerzhinskiy in the VChK: The Confession of a Repentant Chekist”]. *Illustrated Russia*, February 7, 1931.

Dwyer, Jeremy. “Masculinities and Anxieties in the Post-Soviet Boevik Novel.” *Australian Slavonic and Eastern European Studies Journal* 22, no. 1-2 (2008): 1-21.

Dzerzhinskiy, F.E. to I. S. Unshlikht. Telegram dated September 5, 1922, Alexander Yakovlev Archive, http://www.alexanderyakovlev.org/fond/issues-doc/1019506.

Dziak, John. *Chekisty: A History of the KGB.* Lexington, MA: Lexington Books, 1988.

Earley, Pete. *Comrade J: The Untold Secrets of Russia’s Master Spy in America After the End of the Cold War.* New York: Berkley Books, 2007.

Easter, David. “Soviet Bloc and Western Bugging of Opponents’ Diplomatic Premises During the Early Cold War.” *Intelligence and National Security* 31, no. 1 (2016): 28-48, https://www.tandfonline.com/doi/full/10.1080/02684527.2014.926745.

Ebon, Martin. *KGB: Death and Rebirth.* Westport, CT: Praeger, 1994.

Emerson, John B. “Exposing Russian Disinformation.” *Atlantic Council UkraineAlert.* June 29, 2015, https://www.atlanticcouncil.org/blogs/ukrainealert/exposing-russian-disinformation/.

Estonian Foreign Intelligence Service. “How the FSB Signal Intelligence Gathers Information on Foreign Citizens,” in *International Security and Estonia 2019.* Tallinn, Estonia: Välisluureamet, 2019.

Federal Bureau of Investigation. “Comments of Alexander Orlov about Walter Krivitsky’s Book *In Stalin’s Secret Service.*” FBI Memo, October 13, 1954. The National Archives, Kew London, UK, KV 2/2879, serial 45b.

Federal Bureau of Investigation. “Comments by Alexander Orlov Regarding Information Furnished by Walter Krivitsky.” FBI Memo. The National Archives, Kew, London, KV 2/2879, serial 64b, 13.

Federal Bureau of Investigation. “Iosif Volodarsky.” Investigative Summary, The National Archives, Kew, London, KV 2/2881, serial 115a.

Federal Bureau of Investigation. “Valentine Gregory Burtan, Internal Security–R.” Investigative Summary. FBI file 100-262352.

Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency (CISA), and Office of the Director of National Intelligence. “Joint Statement by the Federal Bureau of

Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)." January 5, 2021, https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

Federal Security Service (FSB), Russian Federation. *Военная Контрразведка ФСБ России 1918-2003*, [*Military Counterintelligence of the FSB of Russia, 1918-2003*], Moscow: Moskovskiy Poligraficheskiy Dom, 2003.

Fedor, Julie. "Chekists Look Back on the Cold War: The Polemical Literature." *Intelligence and National Security* 26, no. 6 (December 2011): 842-63.

Felgenhauer, Pavel. "Russia's Imperial General Staff." *Perspective* XVI, no. 1 (October-November 2005). www.bu.ed./iscip/vol16/felgenhauer.

FireEye. *APT28: A Window into Russia's Cyber Espionage Operations?* Milpitas, CA: FireEye, 2014.

Fischer, Ben B., ed. *Okhrana: The Paris Operations of the Russian Imperial Police.* Washington, DC: CIA Center for the Study of Intelligence, 1997.

Fleming, Ian. *From Russia with Love.* London: Penguin, 1957.

Foggo, James, Commander of U.S. Naval Forces Europe. Interview in "On the Horizon: Navigating the European and African Theaters—Episode 14." Commander Sixth Fleet Public Affairs, December 6, 2019. https://www.c6f.navy.mil/Media/transcripts/Article/2043849/on-the-horizon-navigating-the-european-and-african-theaters-episode-14/.

Foreign Intelligence Service of the Russian Federation. "20 Декабря 1920 года" ["20 December 1920"]. http://svr.gov.ru/calendar/6191.htm.

Gabowitsch, Mischa. *Protest in Putin's Russia.* Malden, MA: Polity Press, 2017.

Galeotti, Mark. *Putin's Hydra: Inside Russia's Intelligence Services.* London: European Council on Foreign Relations, 2016. https://ecfr.eu/archive/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf.

Garthoff, Raymond L. *Soviet Leaders and Intelligence: Assessing the American Adversary during the Cold War.* Washington, DC: Georgetown University Press, 2015.

Gavrilov, V. A. *Военная Разведка Информирует: Документы Разведуправления Красной Армии. Январь 1939 – июнь 1941 г.* [*Military Intelligence Informs: Documents from the Red Army Intelligence Directorate. January 1939 – June 1941*]. Moscow: International Democracy Foundation, 2008.

Gerasimov, Valery. "Ценность науки в предвидении: Новые вызовы требуют переосмыслить формы и способы ведения боевых действий" ["The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations"]. *Voyenno-Promyshlennyy Kurier*, February 26, 2013. http://vpk-news.ru/articles/14632.

Giles, Keir. *Russian Ballistic Missile Defense: Rhetoric and Reality.* Carlisle, PA: U.S. Army War College, 2015.

Giles, Keir. *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power.* London: Chatham House Russia and Eurasia Programme, March 2016.

Golubev, S. M. "Операция 'Трест'" ["Operation 'Trust'"], in Yevgeniy Primakov, ed. Очерки Истории Российской Внешней Разведки [*Essays on the History of Russian Foreign Intelligence*], Vol. 2. Moscow: Mezdunarodnye Otnosheniya, 1997. 111-28.

Gorin, Peter. "Black 'Amber': Russian Yantar-Class Optical Reconnaissance Satellites." *Journal of the British Interplanetary Society* 51 (August 1998): 309-20.

Gorin, Peter, "Zenit-The First Soviet Photo-Reconnaissance Satellite," *Journal of the British Interplanetary Society* 50 (November 1997), pp. 441-48.

Gouzenko, Igor. "I Was Inside Stalin's Spy Ring." *Cosmopolitan*. March 1947.

Grenier, Robert. "Spies, Lies and Sneaky Guys: Human INTelligence in the Digital Age." Presentation made for the University of Delaware Global Agenda Speaker Series. March 21, 2012. https://www.youtube.com/watch?v=bfIxarRLMDo.

Harvard Project on the Soviet Social System. Schedule A, Vol. 11, Case 144 (interviewers A.P., and R.B., type A4).

Haynes, John Earl, Harvey Klehr, and Alexander Vassiliev. *Spies: The Rise and Fall of the KGB in America.* New Haven; London: Yale University Press, 2010.

Hendler, Mikhail letter to Congressman Hamilton Fish. Dated November 23, 1930. Richard J. O'Melia Collection, Hesburgh Libraries, University of Notre Dame, Correspondence Box XVI, item 55.

Hendrickx, Bart. "Snooping on Radars: A History of Soviet/Russian Global Signals Intelligence Satellites," *Space Chronicle, Journal of the British Interplanetary Society* 58, Supplement 1 (2005).

Herbig, Katherine L. *Changes in Espionage by Americans: 1947-2007.* Monterey, CA: Defense Personnel Security Research Center, 2008.

Heuer, Richards J., Jr. "Nosenko: Five Paths to Judgment," in H. Bradford Westerfield. *Inside CIA's Private World: Declassified Articles from the Agency 's Internal Journal, 1955-1992.* New Haven: Yale University Press, 1995.

Hopkirk, Peter. *Setting the East Ablaze: Lenin's Dream of an Empire in Asi*a. New York: Kodansha International, 1984.

Howard, Glen E., and Matthew Czekaj, eds. *Russia's Military Strategy and Doctrine.* Washington, DC: The Jamestown Foundation, 2019.

Huang, Christine. "Views of Russia and Putin Remain Negative Across 14 Nations." Pew Research Center, December 16, 2020, https://www.pewresearch.org/fact-tank/2020/12/16/views-of-russia-and-putin-remain-negative-across-14-nations/.

"Ignace Reiss Personal History." Dated October 17, 1949. The National Archives, Kew, London, KV 2/1898, serial 15a.

Institute of Economics and Finance. "Наука и перспективная служба в Вооружённых Силах РФ" ["Science and Perspective Service in the RF Armed Forces"]. March 4, 2019. https://miit-ief.ru/news/nauka-i-perspektivnaya-sluzhba-v-vooruzhyonnyh-silah-rf/.

Jahn, Egbert. "The Castling of Presidential Functions by Vladimir Putin," in *International Politics: Political Issues Under Debate*, Vol. 1. Berlin: Springer, 2015, 107-122.

Jasper, Scott, *Russian Cyber Operations: Coding the Boundaries of Conflict.* Washington, DC: Georgetown University Press, 2020.

Jens, Erik. "Cold War Spy Fiction in Russian Popular Culture: From Suspicion to Acceptance via *Seventeen Moments of Spring.*" *Studies in Intelligence* 62, no. 2 (June 2017): 31-41.

Johnson, Dave. *Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds.* Livermore Papers on Global Security No. 3, Lawrence Livermore National Laboratory, Center for Global Security Research, February 2018.

Joint State Political Directorate (OGPU). "Спецсправка Секретно-политического отдела ОГПУ СССР "О ходе хлебозаготовок в Дальне-Восточном крае" по состоянию на 1 января 1933 г." ["Special Report of the Secret Political Section of the USSR OGPU 'On the Process of Bread Making in the Far Eastern Territory' on Conditions as of 1 January 1993"]. January 13, 1933, Alexander Yakovlev Archive, https://www.alexanderyakovlev.org/fond/issues-doc/1025509.

Jones, Seth, ed. *Moscow's War in Syria.* Washington, DC: Center for Strategic and International Studies, 2020.

Jones, Seth G. "Russian Meddling in the United States: The Historical Context of the Mueller Report." Center for Strategic and International Studies Briefs. March 2019, https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report.

Juurvee, Ivo, and Lavly Perling. *Russia's Espionage in Estonia: A Quantitative Analysis of Convictions.* Tallinn, Estonia: International Centre for Defense and Security, 2019.

Kalugin, Oleg. *Spymaster: My Thirty-Two Years in Intelligence and Espionage Against the West.* New York: Basic Books, 2009.

Kalugin, Oleg Danilovich. *Вид с Лубянки: "Дело" бывшего генерала КГБ* [*The View from Lubyanka: The "Case" of a Former KGB General*]. Moscow: PIK, 1990.

Karavashkin, Vitaliy. *Кто Предал Россию* [*Who Betrayed Russia*]. Moscow: AST, 2008.

Karpov, Petr. Организация ГПУ [*The Organization of the GPU*]. Undated typescript, Hoover Institution Archive, Boris Nicolaevsky Collection, Box 217, Folder 6 (Microfilm reel 187).

Kaznacheev, Alexander. *Inside a Soviet Embassy.* New York: Lippincott, 1962.

Kaznacheyev, Aleksandr Y. "Soviet 'Operation Burma.'" *The New Leader*. January 18, 1960. 41-42.

Kellock-Taschereau Commission. *Report of the Royal Commission Appointed under Order in Council P.C. 411 of February 5, 1946 to Investigate the Facts Relating to and the Circumstances Surrounding the Communication by Public Officials and Other Persons in Positions of Trust of Secret and Confidential Information to Agents of a Foreign Power.* Ottawa: Privy Council, 1946.

Kennan, George. "Telegram to Secretary of State." February 22, 1946. Document 475, in Rogers P. Churchill and William Slany, eds. *Foreign Relations of the United States, The Soviet Union*, Vol. VI. Washington, DC: Government Printing Office, 1969.

Kern, Gary. *A Death in Washington.* New York: Enigma Books, 2003.

KGB Documents Online. https://www.kgbdocuments.eu/kgb-journals-and-books/.

Khaustov, V. N., V. P. Naumov, and N. S. Plotnikova. *Лубянка. Сталин и МГБ. Март 1946 – март 1953: Документы высших органов партийной и государственной власти* [*Lubyanka. Stalin and the MGB March 1946–March 1953: Documents of the Higher Organs of Party and State Power*]. Moscow: International Democracy Foundation, 2007.

Knight, Amy. *Spies without Cloaks: The KGB's Successors.* Princeton: Princeton University Press, 2001.

Knightley, Philip. "Disinformation." *London Review of Books*, July 8, 1993. https://www.lrb.co.uk/the-paper/v15/n13/phillip-knightley/disinformation.

Kocho-Williams, Alastair. *Engaging the World: Soviet Diplomacy and Foreign Propaganda in the 1920s.* University of the West of England, December 2007. https://www2.uwe.ac.uk/faculties/CAHE/HPP/staff/stafflist/A_Kocho-Williams_sovietdiplomats1920s.pdf.

Kofman, Michael. "Russian Performance in the Russo-Georgian War Revisited." *War on the Rocks*, September 4, 2018. https://warontherocks.com/2018/09/russian-performance-in-the-russo-georgian-war-revisited/.

Kofman, Michael, Anya Fink, and Jeffrey Edmonds. *Russian Strategy for Escalation Management: Evolution of Key Concepts.* Arlington, VA: Center for Naval Analysis, 2020.

Kolpakidi, Aleksandr. *Империя ГРУ* [*The GRU Empire*]. Moscow: Olma-Press, 1999. https://www.litmir.me/br/?b=107721.

Korenkov, Sergey A., ed. *Военная Контрразведка ФСБ России 1918-2003* [*Military Counterintelligence of the FSB of Russia, 1918-2003*]. Moscow: Moskovskiy Poligraficheskiy Dom, 2004.

Kouzminov, Alexander. *Biological Espionage: Special Operations of the Soviet and Russian Foreign Intelligence Services in the West.* London: Greenhill Books, 2005.

Kovacevic, Filip. "How Russia Trains its Spies: The Past and Present of Russian Intelligence Education," in Liam Francis Gearon, ed. *The Routledge International Handbook of Universities, Security and Intelligence Studies*. London: Routledge, 2019, 187-95.

Kovacevic, Filip. "Nikolay Dolgopolov: The Storyteller of Soviet Intelligence History." Intelligence and National Security, published online August 13, 2020, https://www.tandfonline.com/doi/abs/10.1080/02684527.2020.1805167.

Kozhevnikov, Yevgeniy. "Work of the Representatives of the 'U.S.S.R.' in China." Forwarded by Shelley to the War Office on June 20, 1927, The National Archives, Kew, London, KV 2/1895, serial 15b.

Kozyrev, Andrey. "Stand By Us." Editorial. *Washington Post*, August 21, 1991. https://www.washingtonpost.com/archive/opinions/1991/08/21/stand-by-us/54b27a33-96b7-4bf2-b8a4-113ddb03f38b/.

Krasnov, Vladislav. *Soviet Defectors: The KGB Wanted List.* Stanford, CA: Hoover Institution Press, 1985.

Krivitsky, Walter G. *I Was Stalin's Agent.* London: Hamish Hamilton, 1939.

Kucharski, Lesley. *Russian Multi-Domain Strategy Against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe.* Livermore, CA: Lawrence Livermore National Laboratory, 2018.

Legvold, Robert. "Review of *Special Tasks: The Memoirs of an Unwanted Witness, A Soviet Spymaster*, by Pavel Sudoplatov and Anatoli Sudoplatov with Jerrold Schechter." *Foreign Affairs* 73, no. 4 (July/August 1994). https://www.foreignaffairs.com/reviews/capsule-review/1994-07-01/special-tasks-memoirs-unwanted-witness-soviet-spymaster.

Lezina, Evgenia. "Dismantling the State Security Apparatus Transformations of the Soviet State Security Bodies in Post-Soviet Russia," in Nikolai Bobrinsky, et al. *Memory of Nations: Democratic Transition Guide: the Russian Experience.* Prague: CEVRO, 2017.

Lipman, Maria. "How Putin Silences Dissent." *Foreign Affairs* 95, no. 3 (May/June 2016): 38-46, https://www.foreignaffairs.com/articles/russia-fsu/2016-04-18/how-putin-silences-dissent.

Logvinenko, Yuriy. *История российского шпионажа и сыска глазами филателиста* [*The History of Russian Espionage and Investigation through the Eyes of a Philatelist*]. Moscow: OLMA Media Group, 2012.

Lovell, David W., and Kevin Windle, eds. "Piecing Together the Past: the Comintern, the CPA, and the Archives," in *Our Unswerving Loyalty: A Documentary Survey of Relations between the Communist Party of Australia and Moscow, 1920-1940.* Canberra: ANU Press, 2008. 1–17.

Main Intelligence Directorate (GRU) of the Soviet Armed Forces General Staff. Moscow to Ottawa, GRU Telegram number 11273, dated August 11, 1945. The National Archives, Kew, London, KV 2/1427, item number 98.

Main Intelligence Directorate (GRU) of the Soviet Armed Forces General Staff. Ottawa to Moscow, GRU Telegram number 209, dated July 12, 1945. The National Archives, Kew, London, KV 2/1247, item 73.

McFadden, David W. "After the Colby Note: The Wilson Administration and the Bolsheviks, 1920-21." *Presidential Studies Quarterly* 25, no. 4 (Fall 1995): 741-50.

McFadden, David W. *Alternative Paths: Soviets and Americans, 1917-1920.* Oxford: Oxford University Press, 1993.

Mendez, Antonio, and Jonna Mendez. *The Moscow Rules: The Secret CIA Tactics that Heled America Win the Cold War.* New York: Hatchette Book Company, 2019.

MI5. Compilation of Ginzberg's MI5 debriefings. "Information Obtained from General Krivitsky during His Visit to This Country, January-February 1940." The National Archives, Kew, London, KV 2/805, serial 55x.

MI5 File on Valentine Gregory Burtan. The National Archives, Kew, London, KV 2/2673.

MI6. "The Corby Case," Secret Intelligence Service summary of Gouzenko interrogations, The National Archives, Kew, London, KV 2/1420.

MI6 Intelligence Reports dated May 23 and May 24, 1933, The National Archives, Kew, London, KV 2/1898, serial 2a.

Ministry of Foreign Affairs of the Russian Federation. *Foreign Policy Concept of the Russian Federation.* December 1, 2016.

Mitrokhin, Vasiliy, ed. *KGB Lexicon: The Soviet Intelligence Officer's Handbook.* London: Frank Cass, 2002.

"Mrs. Petrov's Statement Concerning Her Past Intelligence History," May 15, 1954, National Archives of Australia, A6283, folder 14, item number 4104675, 37-41.

Mueller, Robert S. *The Mueller Report: Report on the Investigation into Russian Interference in the 2016 Presidential Election.* Brooklyn, NY: Melville House, 2019.

Murphy, David, Sergey Kondrashev, and George Bailey. *Battleground Berlin: CIA vs. KGB in the Cold War.* New Haven: Yale University Press, 1997.

National Counterintelligence and Security Center. *Foreign Economic Espionage in Cyberspace.* Washington, DC: NCSC, 2018. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

National Counterintelligence Center. *Annual Report to Congress on Economic Collection and Industrial Espionage.* Washington, DC: NACIC, 1995.

National Cyber Security Centre. "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed." October 3, 2018. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

National Intelligence Council. *The Technology Acquisition Efforts of the Soviet Intelligence Services.* Interagency Intelligence Memorandum, June 1982.

National Security Agency. *Venona*. https://www.nsa.gov/news-features/declassified-documents/venona/.

Nazhestkin, Oleg. "Предисолвия" ["Foreword"], in Yevgeniy Primakov, ed. *Очерки истории российской внешней разведки* [*Essays on the History of Russian Foreign Intelligence*], Vol. 3. Moscow: Mezhdunarodniye Otnosheniya, 2003.

Nehring, Christopher. "Umbrella or Pen? The Murder of Georgi Markov. New Facts and Old Questions." *Journal of Intelligence History* 16, no. 1 (November 22, 2016): 47-58. https://www.tandfonline.com/doi/full/10.1080/16161262.2016.1258248.

Nepomnyashchy, Catharine Theimer. "The Blockbuster Miniseries on Soviet TV: Isaev-Shtirlits, the Ambiguous Hero of *Seventeen Moments of Spring.*" *The Soviet and Post-Soviet Review*, no. 29 (2002): 257-76.

Neumann, Janosh. Interview by Andrew Hammond, Historian of the International Spy Museum, November 12, 2020.

Nikolayev, L. "Суд и Жизнь: 'Судебные Деятели'" ["The Court and Life: 'Judicial Officials'"]. *Soviet Justice Weekly*, April 19, 1923.

Nikolayev, L. "Суд и Жизнь: 'Следователь' Гершуни" ["The Court and Life: 'Inspector' Gershuni"]. *Soviet Justice Weekly*, May 19, 1923.

Nova Scotia Department of Justice. Pre-Sentence Report, "Queen v. Jeffrey Paul Delisle." December 28, 2012. https://assets.documentcloud.org/documents/602196/delisles-pre-sentence-report.pdf.

Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011.* Washington, DC: ONCIX, 2011.

Office of the U.S. Director of National Intelligence. *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Intelligence Community Assessment, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. *Defense Budget Overview: Irreversible Implementation of the National Defense Strategy, United States Department of Defense Fiscal Year 2021 Budget Request.* Washington, DC: Department of Defense, February 2020.

Olmsted, Kathryn S. *Red Spy Queen: A Biography of Elizabeth Bentley.* Chapel Hill, NC: University of North Carolina Press, 2002.

Orlov, Alexander. *Handbook of Intelligence and Guerrilla Warfare.* Ann Arbor: University of Michigan Press, 1963.

Orlov, Alexander. *The Secret History of Stalin's Crimes*. New York: Random House, 1953.

Orlov, Alexander. "The Theory and Practice of Soviet Intelligence." *Studies in Intelligence* 7, no. 1 (Spring 1963): 53-54.

Ovchinnikov, Ivan Vasilyevich. *Исповедь Кулацкого Сына* [*Confession of a Kulak's Son*]. Moscow: Desnitsa, 2000.

Pavlonovsky, Peter (aka Sumarokov). Biography submitted as a statement in his trial in July 1929. Hoover Institution Archive, Boris Nicolaevsky Collection, Box 217, Folder 6 (Microfilm 187).

People's Commissariat for Internal Affairs (NKVD). "Спецсообщение Н.И. Ежова И.В. Сталину с приложением протокола допроса М.Л. Рухимовича" ["Special Report of N. I. Yezhov to J. V. Stalin enclosing the interrogation protocol of M. L. Rukhimovich"]. Alexander Yakovlev Archive. https://www.alexanderyakovlev.org/fond/issues-doc/61283.

Personal History of Hede Massing. Hoover Institution Archive, Hede Massing Papers, Box 1, Folder 1.

Petrov, N. V., and Ya. Foytsik. *Аппарат НКВД-МГБ в Германии. 1945–1953* [*The NKVD-MGB Apparatus in Germany, 1945-1953*]. Moscow: International Democracy Foundation, 2009.

Plekhanov, A. M., and A. A. Plekhanov. *Ф.Э. Дзержинский — Председатель ВЧК-ОГПУ. 1917–1926* [*F. E. Dzerzhinskiy – Chief of the VChK-OGPU 1917-1926*]. Moscow: International Democracy Foundation, 2007.

Plokhy, Serhii. *The Man with the Poison Gun.* London: Oneworld, 2016.

Polgar, Thomas. *The KGB: An Instrument of Soviet Power.* McLean, VA: Association of Former Intelligence Officers, 1989.

Poretsky, Elizabeth. *Our Own People.* Ann Arbor: University of Michigan University Press, 1969.

Prados, John. “The Navy’s Biggest Betrayal.” *Naval History Magazine* 24, no. 3 (June 2010). https://www.usni.org/magazines/naval-history-magazine/2010/june/navys-biggest-betrayal.

Presidium of the Central Committee of the CPSU. “Положение о Комитете государственной безопасности при Совете Министров СССР и его органах на местах” [“Resolution on the Committee of State Security of the USSR Council of Ministers and Its Local Bodies”]. January 9, 1959.

Primakov, Yevgeniy, ed., *Очерки Истории Российской Внешней Разведки* [*Essays on the History of Russian Foreign Intelligence*], 6 vols. Moscow: Mezhdunarodniya Otnosheniya, 1997-2006.

Primakov, Yevgeniy, “Разведка в современном мире” [“Intelligence in the Modern World”]. Speech given to the Journalism Faculty, Moscow State University, October 14, 1992, in Yevgeniy Primakov, ed. *Очерки истории российской внешней разведки* [*Essays on the History of Russian Foreign Intelligence*]. Vol. 6. Moscow: Mezdunarodniya Otnosheniya, 2014.

Prokhorov, Dmitriy *Сколько стоит продать Родину?* [*What is the Cost of Betraying One’s Homeland?*]. Moscow: OLMA-Press, 2005.

Putin, Vladimir. “Being Strong: Why Russia Needs To Rebuild Its Military.” *Foreign Policy*, February 21, 2012, https://foreignpolicy.com/2012/02/21/being-strong/.

Putin, Vladimir. “Поздравление с Днём работника органов безопасности” [“Congratulations on Security Service Workers’ Day”]. Kremlin.ru, December 20, 2020. http://www.kremlin.ru/events/president/news/64681.

Rafalko, Frank J., ed. *CI Reader: American Revolution Into the New Millennium*, Vol 3. Washington, DC: Office of the National Counterintelligence Executive, 2004.

Rastvorov, Yuri. “Red Fraud and Intrigue in the Far East.” *Life*, December 6, 1954. 182.

“Register of Materials Sent to the Director.” Dated January 1945. The National Archives, Kew, London, KV 2/1427, serial 8a, item 108.

“Remarks of Aleksandr Yurievich Kaznacheyev before the Overseas Press Club, New York City,” December 17, 1959, 4, CIA FOIA Reading Room.

Rice, Condoleezza. “The Making of Soviet Strategy,” in Peter Paret, ed. *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Princeton: Princeton University Press, 1986.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare.* New York: Farrar, Straus and Giroux, 2020.

Riehle, Kevin. “Assessing Foreign Intelligence Threats.” *American Intelligence Journal* 31, No. 1 (2013): 96-101. https://www.jstor.org/stable/26202049.

Riehle, Kevin. “The Defector Balance Sheet: Westbound Versus Eastbound Intelligence Defectors from 1945 to 1965.” *International Journal of Intelligence and Counterintelligence* 33, no.

1 (2020): 68-96. https://www.tandfonline.com/doi/abs/10.1080/08850607.2019.1670021?journalCode=ujic20.

Riehle, Kevin. *Soviet Defectors: Revelations of Renegade Intelligence Officers, 1924-1954.* Edinburgh: Edinburgh University Press, 2020.

Riehle, Kevin. "Soviet Intent at the Dawn of the Cold War: Igor Gouzenko's Revelations about GRU Intelligence Taskings." *Journal of Intelligence History*, February 25, 2021. https://www.tandfonline.com/doi/abs/10.1080/16161262.2021.1892997?journalCode=rjih20.

Riehle, Kevin, and Michael May. "Human-cyber Nexus: The Parallels Between 'Illegal' Intelligence Operations and Advanced Persistent Threats," *Intelligence and National Security* 34, no. 2 (2018): 189-204. https://www.tandfonline.com/doi/abs/10.1080/02684527.2018.1534642.

Rostec. Ростех презентует станцию радиотехнической разведки ПОСТ-3М" ["Rostec Presents the POST-3M SIGINT Station"]. Press Release, June 24, 2019.

Russia Foreign Intelligence Service (SVR) website, www.svr.gov.ru.

Russian Federation. "On Countering Terrorism." Article 22, "Lawful Causing of Harm." Federal Law No. 35-F3, June 3, 2006. http://www.consultant.ru/document/cons_doc_LAW_58840/.

Russian Federation. "О внесении изменений в Федеральный закон 'О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера'" ["Amendments to the Federal Law 'On the Defense of the Population and Territory from Extreme Natural or Technological Situations'"]. Federal Law No. 38-F3, March 8, 2015. http://base.garant.ru/70885212/#ixzz6eHSZ0hDq.

Russian Federation. "Questions of Federal Service of the Protection of the Russian Federation." Order of the President of the Russian Federation, August 7, 2004, No. 1013, http://www.consultant.ru/document/cons_doc_LAW_48778/.

Russian Federation, Указ Президента Российской Федерации от 22.10.2007 No. 1404, "О Присвоении Звания Героя Российской Федерации Ковалю Ж.А." [Order of the President of the Russian Federation No. 1404, October 22, 2007, "Awarding the Rank of Hero of the Russian Federation to Koval Zh. A."]. https://rulaws.ru/president/Ukaz-Prezidenta-RF-ot-22.10.2007-N-1404/.

Sakaida, Henry, and Christa Hook. *Heroes of the Soviet Union 1941–45.* Oxford: Osprey Publishing, 2004.

Sakwa, Richard. *Russian Politics and Society.* London: Routledge, 2002.

Savalyev, V. I. "Многоликость Разведки" ["The Many Faces of Intelligence"], in Yevgeniy Primakov, ed. *Очерки Истории Русской Внешней Разведки* [*Essays on the History of Russian Foreign Intelligence*], Vol. 1. Moscow: Mezhdunarodniye Otnosheniya, 1996.

Security Service of Ukraine, Press Center. "SSU Successfully Counteracts Hacker Attacks of Russian Special Services." Press Release, March 13, 2015. http://www.sbu.gov.ua/sbu/control/en/publish/article?art_id=138949&cat_id=35317.

Sherr, James. "Yet Another Reorganization." *Janes Intelligence Review*, August 1, 1995.

Shevchenko, Arkady N. *Breaking with Moscow.* New York: Knopf, 1985.

Sheymov, Victor. *Tower of Secrets: A Real Life Spy Thriller.* Annapolis, MD: Naval Institute Press, 1993.

Sinevirskiy, N. *СМЕРШ: Год в Стане Врага* [*SMERSH: A Year in the Enemy's Camp*]. Limburg an der Lahn, Germany: Possev, 1948; English language publication: Sinevirsky, Nicola. *SMERSH.* New York: Henry Holt, 1950.

Smirnov, Andrey Pavlovich. "Записки агента Разведупра" ["Notes of a Razvedupr Agent"]. *Vozrozhdenie*, March 28, 1930.

Smyslov, O. S. *Генерал Абакумов. Палач или жертва?* [*General Abakumov: Executioner or Victim*]. Moscow: Veche, 2012, online publication. http://www.e-reading.me/chapter.php/1015673/54/Smyslov_-_General_Abakumov._Palach_ili_zhertva.html.

Soldatov, Andrei, and Irina Borogan. *The Compatriots: The Brutal and Chaotic History of Russia's Exiles, Émigrés, and Agents Abroad.* New York: Public Affairs, 2019.

Soldatov, Andrei, and Irina Borogan. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries.* New York: PublicAffairs, 2015.

Spence, Richard B. "Senator William E. Borah: Target of Soviet and Anti-Soviet Intrigue, 1922–1929." *International Journal of Intelligence and CounterIntelligence* 19, no 1 (2006): 134-55.

Stone, Oliver. *The Putin Interviews.* New York: Hot Books, 2017.

Sudoplatov, Pavel. *Спецоперации. Лубянка и Кремль 1930–1950 годы* [*Special Operations: Lubyanka and the Kremlin, 1930-1950*]. Moscow: OLMA-Press, 1997.

Sudoplatov, Pavel. *Special Tasks: The Memoirs of an Unwanted Witness—A Soviet Spymaster*. Boston: Little, Brown and Company, 1994.

Sukovata, Viktoriya. "Evolution of Trauma: Memories of War in Russian Spy Cinema." *Baltic Worlds* 2, no. 2 (2019): 29-36.

Sullivan, Brian R. "Soviet Penetration of the Italian Intelligence Services in the 1930s," in Tomaso Vialardi di Sandigliano and Virgilio Ilari, eds. *The History of Espionage: Italian Military Intelligence, Electronic Intelligence, Chinese Intelligence.* Biella, Italy: Associazione Europea degli Amici degli Archivi Storici, 2005, 83-104.

Suvorov, Viktor. *Aquarium: The Career and Defection of a Soviet Military Spy.* London: Hamish Hamilton, 1985; published in the United States as *Inside the Aquarium: The Making of a Top Soviet Spy.* New York: Stein & Day, 1986.

Suvorov, Viktor. *Inside Soviet Military Intelligence.* New York: MacMillan, 1984.

Suvorov, Viktor. *Spetsnaz: The Inside Story of the Soviet Special Forces.* New York; London: Norton, 1988.

"Testimony of the NKVD Official Zhigunov." German file number EAP 3-a-11/2. National Archives and Records Administration, RG 242, Entry UD 282AV, Box 18.

Thompson, Stephen. "History and Historiography of National Security Space," in Stephen Dick and Roger Launius, eds. *Critical Issues in the History of Spaceflight.* Washington, DC: National Aeronautics and Space Administration, 2006, 481-548.

Trimble, Jeff. "Spreading The Word: The KGB's Image-Building Under Gorbachev." Discussion Paper D-24, The Joan Shorenstein Center, John F. Kennedy School of Government, Harvard University, February 1997.

Trofino, Steffany A. "Dagestan: Moscow's Risk Versus Gain." *International Journal of Intelligence and CounterIntelligence* 24, no. 2 (2011): 253–67.

Trotsky, Lev Davydovich. *Моя Жизнь* [*My Life*], Vol. 2, Berlin: Granit, 1930.

Tumanov, Oleg. *Tumanov: Confessions of a KGB Agent.* Chicago, IL: Edition Q, 1994.

U.S. Army. 441st Counterintelligence Corps (CIC) Detachment Investigative Summary, "REILLY, James Arthur." March 13, 1945. National Archives and Records Administration, RG 319, Entry A1 314B, Box 627.

U.S. Army. Counterintelligence Corps File, "Hans Kukowitsch." National Archives and Records Administration, RG 319, Entry A1 314B, Box 443.

U.S. Army, G2, U.S. Forces Far East. "RASTVOROV, Yurii Alexandrovitch." March 25, 1954, National Archives and Records Administration, RG 319, Entry A1 314B, Box 627

U.S. Army Staff. Investigative Records Repository (Record Group 319).

U.S. Coast Guard Atlantic Area. "Semper Vigilans: History of the USCGC Vigilant (WMEC-617)," https://www.atlanticarea.uscg.mil/Area-Cutters/CGCVIGILANT/History/.

U.S. Congress. House of Representatives, Committee on Foreign Affairs, Subcommittee on State Department Organization and Foreign Operations. *Attempted Defection by Lithuanian Seaman Simas Kudirka.* 91st Congress, Second Session. Washington, DC: Government Printing Office, 1970.

U.S. Congress. Senate, Committee on Foreign Relations. *Russian Intelligence Activities Directed at the Department of State.* 106th Congress, Second Session, February 10, 2000. Washington, DC: Government Printing Office, 2000.

U.S. Congress. Senate, Committee on the Judiciary. *Scope of Soviet Activity in the United States.* 85th Congress, First Session, Part 50. Washington, DC: Government Printing Office, 1957.

U.S. Congress. Senate, Select Committee on Intelligence. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns.* Testimony of Thomas Rid. 115th Congress, March 30, 2017. https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf.

U.S. Department of Justice. "Brooklyn Resident and Two Russian Nationals Arrested in Connection with Scheme to Illegally Export Controlled Technology to Russia." Press Release, October 6, 2016. https://www.justice.gov/opa/pr/brooklyn-resident-and-two-russian-nationals-arrested-connection-scheme-illegally-export.

U.S. Department of Justice. "Evgeny Buryakov Pleads Guilty in Manhattan Federal Court in Connection with Conspiracy To Work for Russian Intelligence." Press Release, March 11, 2016. https://www.justice.gov/usao-sdny/pr/evgeny-buryakov-pleads-guilty-manhattan-federal-court-connection-conspiracy-work.

U.S. Department of Justice. “Exporter of Microelectronics to Russian Military Sentenced to 135 Months in Prison Following Convictions on All Counts at Trial.” Press Release, February 28, 2017, https://www.justice.gov/usao-edny/pr/exporter-microelectronics-russian-military-sentenced.

U.S. Department of Justice. “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.” Press Release, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

U.S. Department of Justice. “Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases (January 2016 to the present: updated January 2019).” January 2019. https://www.hsdl.org/?view&did=825543.

U.S. Department of Justice. “U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts.” Press Release, March 15, 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

U.S. Department of Justice. “U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations.” Press Release, October 4, 2018. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

U.S. Department of Justice. Southern District of New York. “USA vs. Anna Chapman and Mikhail Semenko.” June 27, 2010. https://www.justice.gov/sites/default/files/opa/legacy/2010/06/28/062810complaint1.pdf.

U.S. Department of State. “Department of State Actions in Response to Russian Harassment.” December 29, 2016. https://2009-2017.state.gov/r/pa/prs/ps/2016/12/266145.htm.

U.S. Department of State, Bureau of Public Affairs. *Soviet “Active Measures”: Forgery, Disinformation, Political Operations*, Special Report No. 88, October 1981.

U.S. Department of the Treasury. “Treasury Escalates Sanctions Against the Russian Government’s Attempts to Influence U.S. Elections.” Press Release, April 15, 2021. https://home.treasury.gov/news/press-releases/jy0126.

U.S. Department of the Treasury. “Treasury Sanctions Networks Providing Support to the Government of Syria, Including For Facilitating Syrian Government Oil Purchases from ISIL.” Press Release, November 25, 2015. https://www.treasury.gov/press-center/press-releases/Pages/jl0287.aspx.

U.S. Departments of State and Defense. *The Soviet-Cuban Connection in Central America and the Caribbean.* Washington, DC: U.S. Departments of State and Defense, 1985.

U.S. Director of National Intelligence. *Vision 2015: A Globally Networked and integrated intelligence Enterprise.* Washington, DC: Office of the Director of National Intelligence, 2015. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Vision_2015.pdf.

U.S. District Court, Eastern District of Virginia. "USA v. Peter Rafael Dzibinski Debbins, aka 'Ikar Lesnikov.'" August 20, 2020, https://www.justice.gov/opa/press-release/file/1307186/download.

U.S. District Court, Southern District of Ohio. "USA v. Alexander Yuryevich Korshunov." August 21, 2019. https://www.globalsecurity.org/intell/library/news/2019/intell-190905-doj01_korshunov_complaint.pdf.

U.S. District Court, Western District of Pennsylvania. "USA v. Aleksei Sergeyevich Morenets et al." Case 2:18-cr-00263-MRH, March 10, 2018. https://www.justice.gov/opa/page/file/1098481/download.

U.S. Embassy Havana to Department of State. Despatch 1437, May 25, 1926. National Archives and Records Administration, RG 59, Central Decimal File 1910-1929, Box 7330, Serial 811.00B/585.

U.S. Magistrate Judge, Southern District of New York, "U.S.A. vs. Evgeny Buryakov, aka 'Zenya,' Igor Sporyshev, and Viktor Podobny." January 23, 2015. https://storage.courtlistener.com/recap/gov.uscourts.nysd.438190/gov.uscourts.nysd.438190.1.0.pdf.

U.S. National Archives and Records Administration, Records of the Central Intelligence Agency (Record Group 263).

Ukrtelekom. "Укртелеком офіційно повідомляють про блокування невідомими декількох вузлів зв'язку на півострові" ["Ukrtelekom officially reports blocking of communications nodes on peninsula by unknown actors"]. Press Release, February 28, 2014. http://www.ukrtelecom.ua/presscenter/news/official?id=120327.

Urban, Mark. *The Skripal Files.* London: Pan Books, 2019.

Vassiliev, Alexander. Notebooks. Wilson Center Digital Archive, https://digitalarchive.wilsoncenter.org/collection/86/vassiliev-notebooks.

Velichko, Valeriy. *От Лубянки до Кремля: Секретные Миссии* [*From Lubyanka to the Kremlin: Secret Missions*]. Moscow: Akva-Term, 2013. http://nastural.ru/uploadedFiles/files/biblioteka/Ot_Lubyanki_do_Kremlya._V.Velichko.pdf.

Vershbow, Alexander, NATO Deputy Secretary General. Speech in Trakai, Lithuania. January 15, 2016. https://www.nato.int/cps/en/natohq/opinions_127099.htm.

Vinogradov, V., A. Litvin, and V. Khristoforov, eds. *Архив ВЧК: Сборник документов* [*The VChK Archive: A Collection of Documents*]. Moscow: Kukovo Pole, 2007.

Vorontsov, Sergey A. *Спецслужбы России* [*Special Services of Russia*]. Rostov-na-Donu: Feniks, 2018.

Walker, Christopher. "What is 'Sharp Power'?" *Journal of Democracy* 29, no. 3 (July 2018): 9-23. https://www.journalofdemocracy.org/articles/what-is-sharp-power/.

Walsh, Michael. "George Koval: Atomic Spy Unmasked." *Smithsonian Magazine*, May 2009. https://www.smithsonianmag.com/history/george-koval-atomic-spy-unmasked-125046223/.

Walton, Calder. "Spies, Election Meddling, and Disinformation: Past and Present." *The Brown Journal of World Affairs* 26, no. 1 (Fall/Winter 2019): 107-24. http://bjwa.brown.edu/26-1/spies-election-meddling-and-disinformation-past-and-present/.

Weinstein, Allen, and Alexander Vassiliev. *The Haunted Wood.* New York: Modern Library, 2000.

Weinstein, Marcus. Contact Report dated October 4, 1932. Volodarsky File. The National Archives, Kew, London, KV 2/2880, serial 19a.

Weinstein, Marcus. Contact Report dated October 12, 1932. Volodarsky File. The National Archives, Kew, London, KV 2/2880, serial 21a.

Weiss, Gus W. "The Farewell Dossier: Duping the Soviets." *Studies in Intelligence* 39, no. 5 (1996).

West, Nigel. *Historical Dictionary of Signals Intelligence.* Lanham, MD: Scarecrow Press, 2012.

West, Nigel, and Oleg Tsarev. *The Crown Jewels: The British Secrets at the Heart of the KGB Archives.* New Haven: Yale University Press, 1999.

Westerlund, Fredrik. *Russian Intelligence Gathering for Domestic R&D—Short Cut or Dead End for Modernisation?* Stockholm: Swedish Defence Research Agency, 2010.

Whaley, Barton. *Soviet Clandestine Communication Nets: Notes for a History of the Structures of the Intelligence Services of the USSR.* Cambridge, MA: MIT Center for International Studies, 1969.

Wiebes, Cees, and Przemysław Gasztold. "Polish Intelligence in the Netherlands and Dutch Counter-Intelligence, 1947-1962," *International Journal of Intelligence, Security, and Public Affairs*, published online November 3, 2020. https://www.tandfonline.com/doi/abs/10.1080/23800992.2020.1839726?journalCode=usip20.

Yakovlev, Aleksandr. Database, https://www.alexanderyakovlev.org/db-docs.

Zdanovich, Aleksandr A., and A. G. Bezverkhniy, eds. *Труды Общества Изучения Истории Отечественных Спецслужб* [*Works of the Society for Studying the History of Domestic Special Services*], 3 vols. Moscow: Kuchkove Pole, 2006 and 2007.

Journalist and Blog Articles

Abzalov, Dmitriy. "У ФСО достаточно широкие возможности" ["The FSO Has Broad Enough Opportunities"]. *Kommersant*, September 25, 2016, https://www.kommersant.ru/doc/3154835.

"Alexander Litvinenko: Profile of Murdered Russian Spy." *BBC*, January 21, 2016, https://www.bbc.com/news/uk-19647226.

"Alexei Navalny: Putin Critic Arrives in Germany for Medical Treatment." *BBC*, August 22, 2020, https://www.bbc.com/news/world-europe-53871617.

"Alexei Navalny: Russian opposition leader found guilty." *BBC*, February 8, 2013, https://www.bbc.com/news/world-europe-38905120.

Amos, Howard. "Sergei Magnitsky's posthumous trial gets under way in Russia." *Guardian*, March 22, 2013, https://www.theguardian.com/world/2013/mar/22/sergei-magnitsky-posthumous-trial-russia.

"An Officer and a Diplomat: The Strange Case Of The GRU Spy With A Red Notice," *Bellingcat*, February 25, 2020, https://www.bellingcat.com/news/2020/02/25/an-officer-and-a-diplomat-the-strange-case-of-the-gru-spy-with-a-red-notice/.

Austen, Ian. “Russian Envoys Leave Canada After Officer Is Accused of Spying,” *New York Times*, January 20, 2012, https://www.nytimes.com/2012/01/21/world/americas/russian-diplomats-leave-canada-as-spy-case-heats-up.html.

Balmer, Crispian, and Angelo Amante. “Italy Arrests Navy Captain for Spying, Expels Russian Diplomats.” *Reuters*, March 31, 2021, https://www.reuters.com/article/uk-italy-russia-spies-idAFKBN2BN0W4.

Banse, Dirk, et al. “Circles of Power: Putin’s Secret Friendship with ex-Stasi Officer.” *The Guardian*, August 13, 2014, https://www.theguardian.com/world/2014/aug/13/russia-putin-german-right-hand-man-matthias-warnig.

Baraulina, Anna, Evgenia Pismennaya, and Irina Reznik. “The Great Moscow Bank Shakedown.” *Bloomburg*, December 10, 2019, https://www.bloomberg.com/news/articles/2019-12-10/russia-s-fsb-has-distorted-markets-and-sapped-investment.

Barry, Ellen, and Michael Schwirtz. “Arrests and Violence at Overflowing Rally in Moscow.” *New York Times*, May 6, 2012, https://www.nytimes.com/2012/05/07/world/europe/at-moscow-rally-arrests-and-violence.html.

Baydakova, Anna. “Facial Recognition Tech May Be Being Used Against Russian Protestors.” *Coindesk*, February 1, 2021, https://www.yahoo.com/finance/news/facial-recognition-tech-may-being-213701268.html.

Baynes, Chris. “Russian Spies Found ‘Posing as Plumbers’ in Davos, Report Says.” *Independent*, January 21, 2020, https://www.independent.co.uk/news/world/europe/davos-2020-russia-spies-plumbers-switzerland-wef-a9295076.html.

“Belling the BEAR.” *Threat Connect*, September 28, 2016, https://threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/.

“Berlin Murder: Germany Expels Two Russian Diplomats.” *BBC*, December 4, 2019, https://www.bbc.com/news/world-europe-50659179.

Bershidsky, Leonid. “Putin’s Latest Obsession: A New World War II Narrative” *Bloomberg*, January 10, 2020, https://www.bloomberg.com/opinion/articles/2020-01-10/putin-s-latest-obsession-rewriting-world-war-ii.

Bing, Chris. “APT28 Targeted Montenegro’s Government Before It Joined NATO, Researchers Say,” *Cyberscoop*, June 6, 2017, https://www.cyberscoop.com/apt28-targeted-montenegros-government-joined-nato-researchers-say/.

Blake, Andrew. “Russia-linked Hacking Group Targeting North Americans and European Diplomats: Report,” *AP News*, February 28, 2018, https://apnews.com/article/574b09ffc262cb2edbfce7c4c0f9cd46.

Bodner, Matthew. “Russian Spies May Have Pressured Canadian Union to Get Aircraft Deal.” *Moscow Times*, January 27, 2015, https://www.themoscowtimes.com/2015/01/27/russian-spies-may-have-pressured-canadian-union-to-get-aircraft-deal-a43303.

“Bombardier Sees Delays in Joint-Venture with Russia’s Rostec.” *Reuters*, March 21, 2014, https://www.reuters.com/article/us-bombardier-rostec-idUSBREA2K1ZQ20140321.

Briançon, Pierre. "The Spanish Story of a Russian 'Illegal.'" *Politico*, June 16, 2016, https://www.politico.eu/interactive/the-spanish-story-of-a-russian-illegal-russian-spy-moscow/.

Brodner, Matthew. "The Long Road to Vostochny: Inside Russia's Newest Launch Facility." *Space News*, January 30, 2019, https://spacenews.com/the-long-road-to-vostochny-inside-russias-newest-launch-facility/.

Browne, Ryan. "US and UK Accuse Russia of Major Cyber Attack on Georgia." *CNN*, February 20, 2020, https://www.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html.

"Bulgaria Charges Former Lawmaker With Spying for Russia." *Radio Free Europe/Radio Liberty*, September 10, 2019, https://www.rferl.org/a/bulgaria-charges-former-lawmaker-with-spying-for-russia/30157289.html.

"Bulgaria: Six Arrested Over 'Russian Spy Network.'" DW.com, March 19, 2021, https://www.dw.com/en/bulgaria-six-arrested-over-russian-spy-network/a-56934658.

"Bulgarian NGO Official Charged With Spying for Russia," *Reuters*, September 10, 2019, https://www.reuters.com/article/us-bulgaria-russia-espionage/bulgarian-ngo-official-charged-with-spying-for-russia-idUSKCN1VV1W7.

"Calculate the Value of $1.00 in 1917: What is $1 in 1917 worth in today's money?" Dollar Times, accessed on March 11, 2021, https://www.dollartimes.com/inflation/inflation.php?amount=1&year=1917.

Cenciotti, David. "After the First Tour of duty in February 2016, the Tu-214R Has Returned to Latakia. To Spy on Daesh (and also on the U.S. F-22s?)." *The Aviationist*, July 31, 2016, https://theaviationist.com/2016/07/31/russias-most-advanced-spyplane-has-deployed-to-syria-again/.

Cenciotti, David. "Russia's Most Advanced Spyplane Has Deployed to Syria Again." *Business Insider*, August 1, 2016, https://www.businessinsider.com/russias-most-advanced-spyplane-has-deployed-to-syria-again-2016-8.

Chuter, Andrew. "Russia's Naval Updates Threaten Undersea Comms Network, Says Top British Military Officer." *DefenseNews*, December 15, 2017, https://www.defensenews.com/naval/2017/12/15/russias-naval-updates-threaten-undersea-comms-network-says-top-british-military-officer/.

Cimpanu, Catalin. "German Authorities Charge Russian Hacker for 2015 Bundestag Hack." *Zero Day*, May 5, 2020, https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/.

Cimpanu, Catalin. "Two More Cyber-Attacks Hit Israel's Water System." *Zero Day*, July 20, 2020, https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/.

Cobain, Ian. "Boris Berezovsky Inquest Returns Open Verdict on Death." *Guardian*, March 27, 2014, https://www.theguardian.com/world/2014/mar/27/boris-berezovsky-inquest-open-verdict-death.

Cooney, Peter. "U.S. Concerned by Russian Operations Near Undersea Cables: NY Times." *Reuters*, October 25, 2015, https://www.reuters.com/article/us-usa-security-russia/u-s-concerned-by-russian-operations-near-undersea-cables-ny-times-idUSKCN0SK02G20151026.

Corera, Gordon. "Russia Report: What Would Tougher Spy Laws Mean for UK?" *BBC*, July 22, 2020, https://www.bbc.com/news/uk-53502905.

"CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations." *Dragos*, https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.

"CrowdStrike's Work with the Democratic National Committee: Setting the Record Straight." *CrowdStrike*. June 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Cuthbertson, Anthony. "Chinese and Russian Hackers 'Targeting South Korea Ahead of US-North Korea Summit.'" *Independent*, June 5, 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/trump-us-north-korea-summit-kim-jong-un-hackers-china-russia-a8384586.html.

"(Cyber) GRU (IX): Structure. Other Units." *Lab52.io*, October 8, 2019, https://lab52.io/blog/cyber-gru-ix-structure-other-units/.

Dahlkamp, Jürgen. "No Country More Beautiful." *New York Times*, July 14, 2003, https://www.nytimes.com/2003/07/14/international/europe/no-country-more-beautiful.html.

Dearden, Lizzie. "Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers: Russian energy firms and Danish shipping company also hit by hackers." *Independent*, June 27, 2017, https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html.

Demirjian, Karoun. "Putin denies Russian troops are in Ukraine, decrees certain deaths secret." *Washington Post*, May 28, 2015, https://www.washingtonpost.com/world/putin-denies-russian-troops-are-in-ukraine-decrees-certain-deaths-secret/2015/05/28/9bb15092-0543-11e5-93f4-f24d4af7f97d_story.html.

Dolgopolov, Nikolay. "В разведку на всю жизнь" ("Into Intelligence for Life"). *Rossiyskaya Gazeta*, December 20, 2020, https://rg.ru/2020/03/24/istoriia-razvedchika-mihaila-vasenkova-rassekrechennogo-v-2020-godu.html.

Dorfman, Zach. "How Silicon Valley Became a Den of Spies." *Politico*, July 27, 2018, https://www.politico.com/magazine/story/2018/07/27/silicon-valley-spies-china-russia-219071.

Dorfman, Zach. "The Secret History of the Russian Consulate in San Francisco." *Foreign Policy*, December 14, 2017, https://foreignpolicy.com/2017/12/14/the-secret-history-of-the-russian-consulate-in-san-francisco-putin-trump-spies-moscow/.

Dorfman, Zach, Jenna McLaughlin, and Sean D. Naylor. "Russia carried out a 'stunning' breach of FBI communications system, escalating the spy game on U.S. soil." *Yahoo News*, September 16, 2019, https://news.yahoo.com/exclusive-russia-carried-out-a-stunning-breach-of-fbi-communications-system-escalating-the-spy-game-on-us-soil-090024212.html.

"The Dreadful Eight: GRU's Unit 29155 and the 2015 Poisoning of Emilian Gebrev." Bellingcat, November 23, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/11/23/the-dreadful-eight-grus-unit-29155-and-the-2015-poisoning-of-emilian-gebrev/.

Dunwoody, Matthew, Andrew Thompson, Ben Withnell, Jonathan Leathery, Michael Matonis, and Nick Carr, "Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign." *FireEye*, November 19, 2018, https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html.

"Dutch Diplomat Gets 12 Years for Spying for Russia." *The Moscow Times*, April 22, 2013, https://www.themoscowtimes.com/2013/04/22/dutch-diplomat-gets-12-years-for-spying-for-russia-a23551.

"Dutch Government Says It Disrupted Russian Attempt To Hack Chemical Weapons Watchdog." *CNBC*, October 4, 2018, https://www.cnbc.com/2018/10/04/dutch-government-disrupted-russian-attempt-to-hack-chemical-weapons-watchdog.html.

Eckel, Mike. "Two Decades On, Smoldering Questions About The Russian President's Vault To Power." *Radio Free Europe/Radio Liberty*, August 7, 2019, https://www.rferl.org/a/putin-russia-president-1999-chechnya-apartment-bombings/30097551.html.

Eckel, Mike, Ivan Bedrov, and Olha Komarova. "A Czech Explosion, Russian Agents, a Bulgarian Arms Dealer: The Recipe for a Major Spy Scandal in Central Europe." *Radio Free Europe/Radio Liberty*, April 18, 2021, https://www.rferl.org/a/czech-expulsions-bulgaria-gebrev-russia-gru-intelligence-explosion-spy-scandal/31209960.html.

Egorov, Boris. "5 Legendary Russian Special Forces Units." *Russia Beyond*, November 30, 2018, https://www.rbth.com/science-and-tech/329610-5-legendary-russian-special-forces.

Egorova, Kira, and Ksenia Zubacheva. "The Ruble's Journey Through Time, from the Middle Ages to the Present Day. *Russia Beyond*, May 14, 2020; https://www.rbth.com/business/332176-history-russian-rubl.

Eke, Steven. "Russia Law on Killing 'Extremists' Abroad." *BBC*, November 27, 2006, http://news.bbc.co.uk/2/hi/europe/6188658.stm.

"Electronic Weapons: Yet Another New Russian EW Aircraft." *Strategy Page*, August 28, 2017, https://www.strategypage.com/htmw/htecm/articles/20170818.aspx.

"Emilian Gebrev Assassination Attempt Investigation, 2015." *Bellingcat*, September 4, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/09/04/gebrev-survives-poisonings-post-mortem/.

"EU Targets Syrian Middleman It Says Bought Oil From Islamic State." *Reuters*, March 8, 2015, https://www.reuters.com/article/syria-crisis-eu-idUSL5N0WA05R20150308#1uixRjmfedAEC25e.97.

"Ex-FSB chief: Russian National Guard Creation Important Amid NATO's Eastward Expansion." *TASS*, May 17, 2016, https://tass.com/politics/876141.

"Ex-SoftBank Employee Arrested Over Alleged Leak of Proprietary Information to Russian Spies." *Japan Times*, January 26, 2020, https://www.japantimes.co.jp/news/2020/01/26/national/softbank-employee-arrested-leak-proprietary-information-russia-spies/#.XoyqWtNKgWo

Fein, Esther B. "Soviets Confirm Nazi Pacts Dividing Europe." *New York Times*, August 19, 1989, https://www.nytimes.com/1989/08/19/world/soviets-confirm-nazi-pacts-dividing-europe.html.

Filipov, David. "Putin Thanks Trump for CIA Intel that Foiled a Planned Terrorist Attack in Russia." *Washington Post*, December 17, 2017. https://www.washingtonpost.com/world/putin-thanks-trump-for-cia-intel-that-foiled-a-planned-terrorist-attack-in-russia-the-kremlin-says/2017/12/17/f4274600-e349-11e7-9ec2-518810e7d44d_story.html.

Finkle, Jim. "U.S. Warns Businesses of Hacking Campaign Against Nuclear, Energy Firms." *Reuters*, June 30, 2017, https://www.reuters.com/article/us-usa-cyber-energy/u-s-warns-businesses-of-hacking-campaign-against-nuclear-energy-firms-idUSKBN19L2Z9.

"Flood of Fake Bills is Traced to Russia." *New York Times*, February 24, 1933.

"Former Official Arrested for Treason." *Baltic Times*, September 22, 2008, https://www.baltictimes.com/news/articles/21387/.

Fox, Chris, and Leo Kelion. "Coronavirus: Russian Spies Target Covid-19 Vaccine Research." *BBC News*, July 16, 2020, https://www.bbc.com/news/technology-53429506.

"From Espionage to Cyber Propaganda: Pawn Storm's Activities over the Past Two Years." *TrendMicro*, April 25, 2017, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm.

Fronin, Vyacheslav. "ФСБ расставляет акценты" ["The FSB Sets the Accents"]. *Rossiyskaya Gazeta*, December 19, 2017, https://rg.ru/2017/12/19/aleksandr-bortnikov-fsb-rossii-svobodna-ot-politicheskogo-vliianiia.html.

"Full Analysis of the Sinking of *Liman*." *Planesandstuff*, May 29, 2017, https://planesandstuff.wordpress.com/2017/05/29/full-analysis-of-the-sinking-of-liman/.

"Full Report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia." *Bellingcat*, October 9, 2018, https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/.

"Gas 'Killed Moscow Hostages.'" *BBC*, October 27, 2002, http://news.bbc.co.uk/2/hi/europe/2365383.stm.

"Georgia Accuses Russia of Widespread Cyber Attack." Agenda.ge, February 20, 2020, https://agenda.ge/en/news/2020/535.

"Georgia Says Russian Hackers Block Govt Websites." *Reuters*, August 11, 2008, https://uk.reuters.com/article/us-georgia-ossetia-hackers/georgia-says-russian-hackers-block-govt-websites-idUKLB2050320080811..

"German Man Charged with Giving Bundestag Floor Plans to Russian Intelligence." *Reuters,* February 25, 2021, https://www.reuters.com/article/us-germany-security-russia/german-man-charged-with-giving-bundestag-floor-plans-to-russian-intelligence-idUSKBN2AP11E.

"German Media: Cyber Attack Carried out on Bundestag." *Deutsche Welle*, May 15, 2015, https://www.dw.com/en/german-media-cyber-attack-carried-out-on-bundestag/a-18452770.

"Germany Admits Hackers Infiltrated Federal Ministries, Russian Group Suspected." *Deutsche Welle*, February 28, 2018, https://www.dw.com/en/germany-admits-hackers-infiltrated-federal-ministries-russian-group-suspected/a-42775517.

"Germany Fighting Off Spy Onslaught," *New York Herald Tribune*, October 8, 1961.

Gibbons-Neff, Thomas. "How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria." *New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html.

Gilbert, Caleb (pseudo). "David L. Stern's Phone Talks before Malaysia Airlines Flight 17 Plane Crash." pressbox.co.uk, July 17, 2015.

Gorondi, Pablo. "Hungarian Politician on Trial for Spying on EU for Russia." *AP News*, July 10, 2018, https://apnews.com/article/3fa4f9b515034ab196dbb49fa6e9056e.

Green, J.J. "Assassins Inc.: The Kremlin's Secret Squad of Killers." WTOP.com, October 22, 2018, https://wtop.com/j-j-green-national/2018/10/assassins-inc-the-kremlins-secret-squad-of-killers/.

Greenberg, Andy. "Here's the Evidence That Links Russia's Most Brazen Cyberattacks." *Wired*, November 15, 2019, https://www.wired.com/story/sandworm-russia-cyberattack-links/.

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenberg, Andy. "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History." *Wired*, October 17, 2019, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

Greenberg, Andy. "Your Guide to Russia's Infrastructure Hacking Teams." *Wired*, July 12, 2017, https://www.wired.com/story/russian-hacking-teams-infrastructure/.

Griffin, Andrew. "'Petya' Cyber Attack: Chernobyl's Radiation Monitoring System Hit by Worldwide Hack, Monitoring Is Now Being Performed Manually, Ukrainian Authorities Said." *Independent*, June 27, 2017, https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html.

Grozev, Christo. "FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning." *Bellingcat*, December 14, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/.

Hacquebord, Feike, "Pawn Storm Targets MH17 Investigation Team." *Trendmicro*, October 22, 2015, https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/.

Hall, Louise. "Former Russian PM Describes Trump's Presidency as 'Period of Disappointment.'" *Independent*, February 1, 2021, https://www.independent.co.uk/news/world/americas/us-politics/dmitry-medvedev-trump-presidency-russia-disappointment-b1795684.html.

Halpin, Tony. "Gunmen Kill Seven Women in Russian Sauna." *Times* (London), August 14, 2009.

Hauer, Neil. "Russia's Favorite Mercenaries: Wagner, the Elusive Private Military Company, Has Made Its Way to Africa—with Plenty of Willing Young Russian Volunteers." *The Atlantic*, August 27, 2018, https://www.theatlantic.com/international/archive/2018/08/russian-mercenaries-wagner-africa/568435/.

"Have Russian Hitmen Been Killing With Impunity in Turkey?" *BBC*, December 13, 2016, https://www.bbc.com/news/magazine-38294204.

Hinck, Gregory. "Evaluating the Russian Threat to Undersea Cables," Lawfare Blog, March 5, 2018, https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

Hodge, Nathan, Emma Burrows, and Tara John. "Putin: Sergei Skripal Is a Scumbag and Traitor Who Betrayed Russia." CNN, October 4, 2018, https://www.cnn.com/2018/10/03/europe/putin-calls-skripal-scumbag-intl.

Hodge, Nathan et al. "Russia Detains US Citizen Paul Whelan on Suspicion of Spying." *CNN*, December 31, 2018, https://www.cnn.com/2018/12/31/us/russia-detains-us-citizen/index.html.

Hopkins, Nick. "Suspected Russian Spy Found Working at US Embassy in Moscow." *Guardian*, August 2, 2018, https://www.theguardian.com/us-news/2018/aug/02/suspected-russian-spy-us-embassy-moscow-secret-service.

"How Russia Air Force Jammed Turkish F-16 Aircraft Fighter Jets over Idlib, Syria." *Eurasian Times*, March 9, 2020, https://eurasiantimes.com/how-russian-air-force-jammed-turkish-f-16-fighter-jets-over-idlib-syria/.

"How Russian Spies Bugged the US State Department." *CNN*, October 23, 2019, https://www.cnn.com/2017/08/23/us/spyhunter-russia-bug-us-state-department-declassified/index.html.

"How the Dutch Foiled Russian 'Cyber-Attack' on OPCW." *BBC*, October 4, 2018, https://www.bbc.com/news/world-europe-45747472#share-tools.

Ingram, David. "Democratic Senator Alleges Russian Hackers Unsuccessfully Tried To Access her Computer." NBC News, July 26, 2018, https://www.nbcnews.com/news/us-news/democratic-senator-alleges-russian-hackers-unsuccessfully-tried-access-her-computer-n895131.

"Introducing WhiteBear." Kaspersky SecureList, August 30, 2017, https://securelist.com/introducing-whitebear/81638/.

Jauvert, Vincent. "Révélations sur les espions russes en France" ["Revelations about Russian Spies in France"]. L'Obs.com, July 24, 2014.

Jones, Jeffrey M. "Fewer in U.S. Regard China Favorably or as Leading Economy." Gallup, March 2, 2020, https://news.gallup.com/poll/287108/fewer-regard-china-favorably-leading-economy.aspx.

Jozwiak, Rikard, "EU Lawmakers Say Russia Using Coronavirus Crisis for Political Benefit." *RFE/RL*, April 3, 2020. https://www.rferl.org/a/eu-lawmakers-say-russia-using-coronavirus-crisis-to-gain-political-benefits/30529085.html.

Kantouris, Costas, and Menelaos Hadjicostis. "Greece: Russians Expelled Over Cash-for-Protests Allegation." *AP News*, July 12, 2018, https://apnews.com/article/aaf032985e7341d3a7968f6ff6b95ce0.

"K.G.B. Passes Secrets Back to U.S." *New York Times*, December 14, 1991.

Khazov-Kassia, Sergey. "Человек за Спиной" ["The Man Behind the Back"]. *New Times*, November 17, 2014, https://newtimes.ru/articles/detail/90102.

Khrolenko, Aleksandr. "Военный бюджет США: что достанется Латвии" ["The US Defense Budget: What does Latvia Get"]. Sputniknews.ru, February 12, 2020.

Khrushcheva, Nina. "Последний силовик?" ["The Latest Silovik?"]. Inosmi.ru, December 4, 2017, https://inosmi.ru/politic/20171204/240916440.html.

Khurshudyan, Isabelle. "Putin Thanks Trump for Information That He Says Helped Foil a Planned Terrorist Attack in St. Petersburg." *Washington Post*, December 30, 2019, https://www.washingtonpost.com/world/putin-thanks-trump-for-information-that-helped-foil-a-planned-terrorist-attack-in-st-petersburg/2019/12/30/9788ee34-2b32-11ea-bffe-020c88b3f120_story.html.

Kolesnikov, Andrey. "ФСБ, Устремленная в Будущее" ["The FSB, Looking to the Future"]. *New Times*, February 19, 2018, https://newtimes.ru/articles/detail/147619.

"Kondor Spacecraft Overview." SpaceFlight101.com, 2020, https://spaceflight101.com/spacecraft/kondor/.

Korzun, A., and V. Filin. "Stirlits Worked at the 'Aquarium': 13 Little Known Facts from the Life of the Main Intelligence Directorate." *Komsomolskaya Pravda*, October 10, 1992, translated by the Foreign Broadcast Information Service, Central Asia, Military Affairs, JPRS-UMA-92-044, December 9, 1992.

Krutikov, Yevgeniy. "Российская нелегальная разведка остается предметом зависти Запада" ["Russian Illegal Intelligence Remains an Object of Envy in the West"]. *Vzglyad*, July 29, 2007, https://vz.ru/politics/2017/6/29/876627.html.

Kudryavtsev, Aleksandr. "Генерал Армии Виктор Золотов: 'Росгвардия Работает Для Людей'" ["Army General Viktor Zolotov: 'Rosgvardiya Works for the People'"]. *Voenniy*, no. 4 (2017), https://rosguard.gov.ru/ru/page/index/zhurnal-voennyj-4-general-armii-viktor-zolotov-rosgvardiya-rabotaet-dlya-lyudej.

"The Labor Party Exposed to Hostile Hacker Attacks." TV2.no, February 2, 2017, https://www.tv2.no/nyheter/8902520/.

LaGrone, Sam. "Coast Guard: Russian Surveillance Ship Operating in 'Unsafe' Manner off East Coast." *USNI News*, December 17, 2019, https://news.usni.org/2019/12/17/coast-guard-russian-surveillance-ship-operating-in-unsafe-manner-of-east-coast.

Lee, Victor Robert. "Satellite Images: A (Worrying) Cuban Mystery." *The Diplomat*, June 8, 2018, https://thediplomat.com/2018/06/satellite-images-a-worrying-cuban-mystery/.

Leventhal, Todd. "Traffic in Baby Parts Has No Factual Basis." *New York Times*, February 26, 1992.

Lewis, Jason. "Mikhail Repin: The Perfect Party Guest Who Was Whitehall Spy for the Russians." *Telegraph,* December 10, 2011, https://www.telegraph.co.uk/news/worldnews/europe/russia/8948357/Mikhail-Repin-the-perfect-party-guest-who-was-Whitehall-spy-for-the-Russians.html.

Lewis, Jason. "Russian Spy Targeted MPs and Whitehall Officials." *Telegraph*, December 10, 2011, https://www.telegraph.co.uk/news/worldnews/europe/russia/8948359/Russian-spy-targeted-MPs-and-Whitehall-officials.html.

Lewis, Jason. "The Traitor in a Headscarf: How Czech Spy Agent Hammer Worked Secretly Inside Parliament for Years." *Daily Mail*, November 15, 2008, https://www.dailymail.co.uk/news/article-1086187/The-traitor-headscarf-How-Czech-spy-Agent-Hammer-worked-secretly-inside-Parliament-years.html.

Leyden, John. "Ukraine Claims It Blocked VPNFilter Attack at Chemical Plant," theregister.co.uk, July 13, 2018, https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/.

"Liana Electronic Intelligence Program" SpaceFlight101.com, 2020, http://spaceflight101.com/spacecraft/liana-electronic-intelligence-program/.

"Lithuanian Court Upholds Sentence for Man Convicted of Spying for Russia." LRT.lt, January 17, 2020, https://www.lrt.lt/en/news-in-english/19/1134237/lithuanian-court-upholds-sentence-for-man-convicted-of-spying-for-russia.

Litvinova, Daria. "Navalny Releases Recording of Call to his Alleged Poisoner." *AP News*, December 21, 2020, https://apnews.com/article/alexei-navalny-poisoning-underpants-202f470c2d1c19151b9deb564d94e8f9.

Lyngaas, Sean. "Russian Intelligence-Backed Hackers Go After Armenian Embassy Website with New Code." *Cyberscoop*, March 12, 2020, https://www.cyberscoop.com/turla-fsb-eset-armenia/.

MacFarquhar, Neil. "A Powerful Russian Weapon: The Spread of False Stories." *New York Times*, August 28, 2016, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

"Maria Butina: The Russian Gun Activist who Was Jailed in the US." *BBC*, October 25, 2019, https://www.bbc.com/news/world-us-canada-44885633.

Masters, James. "Theresa May's Full Statement on Russian Spy's Poisoning." *CNN*, March 13, 2018, https://www.cnn.com/2018/03/13/europe/theresa-may-russia-spy-speech-intl/index.html.

McIntire, Mike. "Billionaire Backer of Maria Butina Had Russian Security Ties." *New York Times*, September 21, 2018, https://www.nytimes.com/2018/09/21/us/politics/maria-butina-russian-oligarch.html.

Mcquade, Dan. "Russian Spy Ship Spotted Off Coast of Delaware." Phillymag.com, February 14, 2017, https://www.phillymag.com/news/2017/02/14/russian-spy-ship-delaware-coast/.

"Media: podejrzany o szpiegostwo na rzecz Rosji pracował w Agencji Mienia Wojskowego" ["Media: The Person Arrested for Espionage for Russia Worked in the Agency of Military

Property"]. *Polskie Radio*, October 28, 2019, https://polskieradio24.pl/5/1222/Artykul/2392622,ABW-zatrzymala-Piotra-S-Jest-podejrzany-o-szpiegostwo-na-rzecz-Rosji.

Meyer, Josh. "Accused Russian Agent Met with Suspected Kremlin Spy." *Politico*, July 28, 2018, https://www.politico.com/story/2018/07/28/mariia-butina-russia-kremlin-suspected-spy-746043.

Meyers, Adam. "CrowdStrike's January Adversary of the Month: VOODOO BEAR," *CrowdStrike*, January 29, 2018, https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/.

Meyers, Adam. "Meet CrowdStrike's Adversary of the Month for March: VENOMOUS BEAR." *CrowdStrike*, March 12, 2018, https://www.crowdstrike.com/blog/meet-crowd strikes-adversary-of-the-month-for-march-venomous-bear/.

Modderkolk, Huib. "Dutch Agencies Provide Crucial Intel about Russia's Interference in US-Elections." *deVolkskant*, January 25, 2018, https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/.

"Montenegro Jails 'Russian Coup Plot' Leaders." *BBC*, May 9, 2019, https://www.bbc.com/news/world-europe-48212435.

Mooney, John. "Russian Agents Plunge to New Ocean Depths in Ireland to Crack Transatlantic Cables." *Sunday Times*, February 16, 2020, https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz.

Morris, Loveday, and Robyn Dixon. "Bulgaria Alleges Russian Links to Arms Depot Blasts, Widening European Probes into Moscow Agents." *Washington Post*, April 28, 2021, https://www.washingtonpost.com/world/europe/bulgaria-russia-arms-explosions-czech-republic/2021/04/28/ba2e7004-a812-11eb-a8a7-5f45ddcdf364_story.html.

Morris, Loveday, Ladka Bauerova, and Robyn Dixon. "Accusations of Spying and Sabotage Plunge Russian-Czech Relations into the Deep Freeze." *Washington Post*, April 19, 2021, https://www.washingtonpost.com/world/europe/russia-diplomats-expulsions-czech/2021/04/19/ef7f6178-9fbb-11eb-b2f5-7d2f0182750d_story.html.

Mortkowitz, Siegfried. "Czechs Expel More Russian Embassy Staff Over Bombing Claims." *Politico*, April 22, 2021, https://www.politico.eu/article/czech-republic-russia-embassy-staff-bombing-claims/.

Nakashima, Ellen, and Craig Timberg. "Russian Government Hackers Are Behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce." *Washington Post*, December 14, 2020, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

Nardelli, Alberto. "The EU's Embassy in Russia Was Hacked but the EU Kept It a Secret." *BuzzFeed*, June 5, 2019, https://www.buzzfeednews.com/article/albertonardelli/eu-embassy-moscow-hack-russia.

Nechepurenko, Ivan. "New Spies Went for a Joyride in Moscow. Russia Isn't Happy." *New York Times*, July 14, 2016, https://www.nytimes.com/2016/07/15/world/europe/russia-fsb-security-service.html.

Nemtsova, Anna. "A Chill in the Moscow Air." *Newsweek*, February 5, 2006, https://www.newsweek.com/chill-moscow-air-113415.

Nemtsova, Anna, and Thomas Seibert. "Russia's ISIS Money Men Exposed." *The Daily Beast*, June 26, 2017, https://www.thedailybeast.com/russias-isis-money-men-exposed?ref=scroll.

Neuman, Scott. "Ukraine To Expel Russian Diplomat Caught Taking Classified Info." *NPR*, May 1, 2014, https://www.npr.org/sections/thetwo-way/2014/05/01/308605849/ukraine-to-expel-russian-diplomat-caught-taking-classified-info.

Nikolskaya, Polina, and Darya Korsunskaya. "Russian Ex-minister Ulyukayev Jailed for Eight Years over $2 Million Bribe." *Reuters*, December 15, 2017, https://www.reuters.com/article/us-russia-ulyukayev-verdict/russian-ex-minister-ulyukayev-jailed-for-eight-years-over-2-million-bribe-idUSKBN1E90SN.

Nilsen, Thomas. "Video: Norway's New F-35 Filmed from Russian Anti-submarine Plane." *Barents Observer*, March 10, 2020, https://thebarentsobserver.com/en/security/2020/03/video-norways-new-f-35-filmed-russian-anti-submarine-plane.

Nimmo, Ben. "How MH17 Gave Birth to the Modern Russian Spin Machine." *Foreign Policy*, September 29, 2016, https://foreignpolicy.com/2016/09/29/how-mh17-gave-birth-to-the-modern-russian-spin-machine-putin-ukraine/.

Olsen, Jan M. "Norway says Russia was behind hacker attack on parliament." *AP News*, October 14, 2020, https://apnews.com/article/technology-oslo-russia-denmark-hacking-4c177f74287ab69816b954f8793e26c1.

Olsen, Jan M., and Desmond Butler. "Russian Diplomat Accused of Espionage Quietly Leaves Sweden." *US News and World Report*, March 28, 2019.

Operov, Sergey, and Ivan Safronov. "Министерство чрезвычайных полномочий: Готовится реформа правоохранительных и силовых структур" ["Ministry of Emergency Powers: A Reform of Law Enforcement and Power Structures is Being Prepared"]. *Kommersant*, June 19, 2016, https://www.kommersant.ru/doc/3093174.

Osborne, Charlie. "Russian APT Turla Targets 35 Countries on the Back of Iranian Infrastructure." *Zero Day*, October 21, 2019, https://www.zdnet.com/article/russian-apt-turla-targets-35-countries-on-the-back-of-iranian-infrastructure/.

Ostroukh, Andrey. "Russia's Putin Signs NGO 'Foreign Agents' Law." *Reuters*, July 21, 2012, https://www.reuters.com/article/us-russia-putin-ngos/russias-putin-signs-ngo-foreign-agents-law-idUSBRE86K05M20120721.

Ostrower, Jon, and Paul Vieira. "Bombardier Shelves Plans for Russian Assembly Line." *Wall Street Journal*, October 30, 2014, https://www.wsj.com/articles/bombardier-shelves-plans-for-russian-assembly-line-1414699181.

"Ottawa Denies Soviet Spy Defected Here." *The Gazette* (Montreal), March 27, 1972.

Owen, Glen. "Labour MP Pulled Before Chief Whip for Inviting 'Russian Spy' to Tea in the Commons." *Daily Mail*, June 28, 2008, https://www.dailymail.co.uk/news/article-1030235/Labour-MP-pulled-chief-whip-inviting-Russian-spy-tea-Commons.html.

Perlroth, Nicole. "Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid." *New York Times*, October 24, 2020, https://www.nytimes.com/2020/10/23/us/politics/energetic-bear-russian-hackers.html.

Polantz, Katelyn, Veronica Stracqualursi, and Marshall Cohen. "Alleged Russian Spy Maria Butina Pleads Guilty to Engaging in Conspiracy against US." *CNN*, December 13, 2018, https://www.cnn.com/2018/12/13/politics/maria-butina-guilty-plea/index.html.

Polityuk, Pavel. "Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid." *Reuters*, December 20, 2016, https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF.

Polityuk, Pavel, and Alessandra Prentice. "Ukrainian Banks, Electricity Firm Hit by Fresh Cyber Attack." *Reuters*, June 27, 2017, https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ.

Polovinko, Vyacheslav, and Lilit Sarkisyan. "The FSB Gathers Up the Keys to 'Yandex.'" *Novaya Gazeta*, June 5, 2019.

"Profile: Mikhail Khodorkovsky." *BBC*, December 22, 2013, https://www.bbc.com/news/world-europe-12082222.

Prothero, Mitch. "'Unit 29155': Putin's Assassination Squad—Suspected of Killings all over Europe—Received Diplomatic Cover from the Russian Mission in Switzerland." *Business Insider*, March 16, 2020, https://www.businessinsider.com/unit-29155-assassination-squad-diplomatic-russia-mission-switzerland-2020-3.

"Public Diplomacy's 90th Anniversary at RCSC." *Russian Beyond*, November 20, 2015, https://www.rbth.com/arts/culture/2015/11/20/public-diplomacys-90th-anniversary-at-rcsc_542417.

"Putin Stresses Importance of New Far East Space Center." *RIA Novosti*, August 28, 2010.

"Record $185M in Cash Seized From Russian Official in Sting Operation." *Moscow Times*, May 20, 2019, https://www.themoscowtimes.com/2019/05/20/185m-seized-from-ex-fsb-official-in-corruption-scandal-a65658.

Reevell, Patrick. "How Russia Is Using Facial Recognition To Police Its Coronavirus Lockdown." *ABC News*, April 30, 2020, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736.

Remnick, David. "KGB Targeted for Major Reform." *Washington Post*, August 27, 1991.

"The Rise and Fall of an FSB-Run Money Laundering Empire." *Moscow Times*, August 3, 2019, https://www.themoscowtimes.com/2019/08/03/the-rise-and-fall-of-an-fsb-run-money-laundering-empire-a67226.

"Rookie FSB Agents Are Punished for 'Indecent' Graduation Jinx in Moscow." *Siberian Times*, August 2, 2016, https://siberiantimes.com/home/sent-to-siberia/s0025-rookie-fsb-agents-are-punished-for-indecent-graduation-jinx-in-moscow/.

Rosenberg, Steven. "Ukraine Crisis: Meeting the Little Green Men." *BBC*, April 30, 2014, https://www.bbc.com/news/world-europe-27231649.

Roth, Andrew. "Vladimir Putin Calls Sergei Skripal a Scumbag and a Traitor." *Guardian*, October 3, 2018, https://www.theguardian.com/uk-news/2018/oct/03/vladimir-putin-calls-sergei-skripal-a-scumbag-and-traitor.

"Russia Assassinated at least 13 Chechens Abroad Before Victim Returned Fire in Kyiv." *Euro-Maidan Press*, June 21, 2017, http://euromaidanpress.com/2017/06/21/russia-assassinated-at-least-14-chechens-abroad-before-it-failed-on-osmayev/.

"Russia: 'Big Brother' Law Harms Security, Rights." *Human Rights Watch*, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

"Russia Blames Israel after Military Plane Shot Down off Syria." *BBC*, September 18, 2018, https://www.bbc.com/news/world-europe-45556290.

"Russia Considers Stronger Secrecy Laws." *Financial Times*, October 30, 2015, https://www.ft.com/content/fc155bca-7f25-11e5-98fb-5a6d4728f74e.

"Russia 'Ends Chechnya Operation'," *BBC*, April 16, 2009, http://news.bbc.co.uk/2/hi/europe/8001495.stm.

"Russia Sends New Intelligence Cadres to Its Embassy in Vilnius–Investigation." LRT.lt, August 29, 2019, https://www.lrt.lt/en/news-in-english/19/1092698/russia-sends-new-intelligence-cadres-to-its-embassy-in-vilnius-investigation.

"Russia to Install 'Orwell' Facial Recognition Tech in Every School." *Moscow Times*, June 16, 2020, https://www.themoscowtimes.com/2020/06/16/russia-to-install-orwell-facial-recognition-tech-in-every-school-vedomosti-a70585.

"Russia's Brain Drain on the Rise over Economic Woes—Report." *Moscow Times*, January 24, 2018, https://www.themoscowtimes.com/2018/01/24/russias-brain-drain-on-the-rise-over-economic-woes-report-a60263.

"Russia's Decision To Close Down Gabala Radar Station Is Final—Lavrov." *Interfax*, January 23, 2013, https://www.rbth.com/news/2013/01/23/russias_decision_to_close_down_gabala_radar_station_is_final_-_lavrov_pa_22129.html.

"Russia's FSB Disciplines Future Officers Over SUV Parade Stunt." *Radio Free Europe/Radio Liberty*, July 14, 2016, https://www.rferl.org/a/russia-fsb-future-officers-disciplined-parade-stunt/27858804.html.

"Russia's Rostec in Joint Venture Talks with Bombardier." *Reuters*, February 15, 2013, https://www.reuters.com/article/us-russia-rostec-bombardier/russias-rostec-in-joint-venture-talks-with-bombardier-idUSBRE91E0BW20130215.

"Russia's Ships, Missile Systems Put on Duty Due to NATO Exercise in Black Sea." *TASS*, April 8, 2019, https://tass.com/defense/1052558.

"Russian Ex-minister Ulyukayev Gets Eight Years for Bribery." *BBC*, December 15, 2017, https://www.bbc.com/news/world-europe-42365041.

"Russian Hackers Leak Simone Biles and Serena Williams Files." *BBC*, September 13, 2016, https://www.bbc.com/news/world-37352326.

"Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say." *Wall Street Journal*, July 23, 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110.

"Russian Long-range radar in Belarus To Track U.S. Missile Defense System in Europe." Belta.by, February 15, 2012, .

"Russian Mole Had Access to Wealth of CSIS, RCMP, Privy Council files." *The Globe and Mail*, October 22, 2012, https://www.theglobeandmail.com/news/politics/russian-mole-had-access-to-wealth-of-csis-rcmp-prive-council-files/article4627659/.

"Russian Official: We Are Working on Reopening Cuba, Vietnam Bases." Voice of America, October 7, 2016, https://www.voanews.com/europe/russian-official-we-are-working-reopening-cuba-vietnam-bases..

"Russian 'Spy' Katia Zatuliveter: MP Lover Paid for Trips." *BBC*, October 27, 2011, https://www.bbc.com/news/uk-15476077.

"Russian 'Spy' Moved from Prison to House Arrest." *The Italian Insider*, December 3, 2019.

"Russian spy Raymond Poeteray jailed by Dutch." *BBC*, April 23, 2013, https://www.bbc.com/news/world-europe-22265494.

"Russians Warned To Keep Vigilant; 'Capitalist Encirclement' Still Continues, Says Pravda in Urging Stronger Defenses." *New York Times*, March 19, 1953.

Ryan, Missy. "Russian, Syrian Partnership Poses a new Challenge for U.S. in Iraq." *Washington Post*, September 28, 2015, https://www.washingtonpost.com/world/national-security/russian-syrian-partnership-poses-a-new-challenge-for-us-in-iraq/2015/09/28/b1190982-65ee-11e5-9223-70cb36460919_story.html.

Ryan, Missy, and Sudarsan Raghavan. "Russians Arrested as Spies in Libya Worked for Russian firm Wagner, Official Says." *Washington Post*, November 18, 2019, https://www.washingtonpost.com/world/national-security/russians-arrested-as-spies-in-libya-worked-for-russian-firm-wagner-official-says/2019/11/18/c0cee91a-0a21-11ea-a49f-9066f51640f6_story.html.

Ryan, Missy, Ellen Nakashima, and Karen DeYoung. "Obama administration announces measures to punish Russia for 2016 election interference." *Washington Post,* December 29, 2016, https://www.washingtonpost.com/world/national-security/obama-administration-announces-measures-to-punish-russia-for-2016-election-interference/2016/12/29/311db9d6-cdde-11e6-a87f-b917067331bb_story.html.

Saad, Lydia. "Majority of Americans Now Consider Russia a Critical Threat." Gallup, February 27, 2019, https://news.gallup.com/poll/247100/majority-americans-consider-russia-critical-threat.aspx.

Safire, William. "Who Lost Mount Alto." *New York Times*, September 22, 1985.

Salikhov, Aleksandr. "От Региступра до ГРУ: путь длиной в 88 лет" ["From Registupr to GRU: The 88-year Journey"]. Chekist.ru, March 31, 2006. chekist.ru/article/1326.

Saradzhyan, Simon, and Carl Schreck. "NGOs a Cover for Spying in Russia." Globasresearch.ca, May 13, 2005, https://www.globalresearch.ca/ngos-a-cover-for-spying-in-russia/139.

Sauer, Pjotr. "In Push for Africa, Russia's Wagner Mercenaries Are 'Out of Their Depth' in Mozambique." *Moscow Times*, November 19, 2019, https://www.themoscowtimes.com/2019/11/19/in-push-for-africa-russias-wagner-mercenaries-are-out-of-their-depth-in-mozambique-a68220.

"SBU Thwarts Cyber Attack from Russia Against Chlorine Station in Dnipropetrovsk Region." *Interfax-Ukraine*, July 11, 2018, https://en.interfax.com.ua/news/general/517337.html.

Schreck, Carl. "FBI Wary of Possible Russian Spies Lurking in U.S. Tech Sector." *Radio Free Europe/Radio Liberty*, May 17, 2014, https://www.rferl.org/a/fbi-wary-of-possible-russian-spies-in-lurking-in-us-tech-sector/25388490.html.

Schreck, Carl. "From 'Not Us' To 'Why Hide It'?: How Russia Denied Its Crimea Invasion, Then Admitted It." *Radio Free Europe/Radio Liberty*, February 26, 2019, https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html.

Schudel, Matt. "Victor Sheymov, KGB officer Who Defected From Soviet Union, Dies at 73." *Washington Post*, December 5, 2019, https://www.washingtonpost.com/local/obituaries/victor-sheymov-kgb-officer-who-defected-from-soviet-union-dies-at-73/2019/12/05/e773a22c-16b5-11ea-a659-7d69641c6ff7_story.html.

Schwirtz, Michael. "Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say." *New York Times*, October 8, 2019, https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html.

"Seven FSB officials Have Been Arrested in a Robbery Case. They May Have Also Stolen Money During Searches of Corrupt Officials," *Meduza*, July 5, 2019, https://meduza.io/en/feature/2019/07/05/seven-fsb-officials-have-been-arrested-in-a-robbery-case-they-may-have-also-stolen-money-during-searches-of-corrupt-officials.

Shalal, Andrea. "German Intelligence Sees Russia Behind Hack Of Energy Firms: Media Report." *Reuters*, June 20, 2018, https://www.reuters.com/article/us-germany-cyber-russia/german-intelligence-sees-russia-behind-hack-of-energy-firms-media-report-idUSKBN1JG2X2.

Shalal, Andrea. "Russia-Germany Gas Pipeline Raises Intelligence Concerns—U.S. Official." *Reuters*, May 17, 2018, https://uk.reuters.com/article/uk-usa-germany-russia-pipeline/russia-germany-gas-pipeline-raises-intelligence-concerns-u-s-official-idUKKCN1II0V7.

Shane, Scott, David E. Sanger, and Andrew E. Kramer. "Russians Charged with Treason Worked in Office Linked to Election Hacking." *New York Times*, January 27, 2017, https://www.nytimes.com/2017/01/27/world/europe/russia-hacking-us-election.html.

Shelbourne, Mallory. "No Russian or Chinese Presence at First Week of RIMPAC." *USNI News*, August 24, 2020, https://news.usni.org/2020/08/24/no-russian-or-chinese-presence-at-first-week-of-rimpac.

Singgih, Viriya, Arys Aditya, and Karlis Salna. "Indonesia Says Election Under Attack from Chinese, Russian Hackers." *Bloomberg*, March 13, 2019, https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers.

Sinodov, Yuriy. "Грязные руки" ["Dirty Hands"]. Roem.ru, July 18, 2011, https://roem.ru/18-07-2011/120190/gryaznye-ruki/.

Sixto, Daniel. "Russian Mercenaries: A String of Failures in Africa." *Geopolitical Monitor*, August 24, 2020, https://www.geopoliticalmonitor.com/russian-mercenaries-a-string-of-failures-in-africa/.

"Skripal Suspect Boshirov Identified as GRU Colonel Anatoliy Chepiga." *Bellingcat*, September 26, 2018, https://www.bellingcat.com/news/uk-and-europe/2018/09/26/skripal-suspect-boshirov-identified-gru-colonel-anatoliy-chepiga/.

"Slovak PM Says Russian Diplomat Expelled for Spying." *Radio Free Europe/Radio Liberty*, December 5, 2018, https://www.rferl.org/a/slovak-pm-says-russian-diplomat-expelled-for-spying/29639128.html.

Smith, Ben. "Clinton Friend Was Spy's Target." *Politico*, June 29, 2010, https://www.politico.com/blogs/ben-smith/2010/06/clinton-friend-was-spys-target-027850.

Soldatkin, Vladimir, and Christian Lowe. "Russia Orders out 60 U.S. Diplomats over Spy Poisoning Affair." *Reuters*, March 20, 2018, https://www.reuters.com/article/us-russia-diplomats/russia-orders-out-60-u-s-diplomats-over-spy-poisoning-affair-idUSKBN1H52MN.

Somers, Sue. "Ik vind nietdat ik iets anti-Belgisch heb gedaan" ["I Don't Think I've Done Anything Anti-Belgian"]. *DeMorgen*, July 16, 2011, https://www.demorgen.be/nieuws/ik-vind-nietdat-ik-iets-anti-belgisch-heb-gedaan~b95a6b30/.

"Spies Without Borders—How the FSB Infiltrated the International Visa System." *Bellingcat*, November 16, 2018, https://www.bellingcat.com/news/uk-and-europe/2018/11/16/spies-without-borders-fsb-infiltrated-international-visa-system/.

Staalesen, Atle. "Mikhail Bochkarev Is Released, Norwegian Security Police Might Drop Espionage Charges." *Barents Observer*, October 19, 2018, https://thebarentsobserver.com/en/life-and-public/2018/10/mikhail-bochkarev-released-norwegian-security-police-drops-espionage-charges.

Stillwell, Blake. "This US Army Sergeant Started the Korean War by Selling Out to the Soviets." *Business Insider*, May 24, 2016.

Stone, Laura. "Canadian Diplomat Expelled from Russia." *Global News*, April 22, 2014, https://globalnews.ca/news/1284073/canadian-diplomat-expelled-from-russia/.

Sukhankin, Sergey. "Russian National Guard: A New Oprichnina, 'Cyber Police' or Something Else?" *Eurasia Daily Monitor* 14, no. 38 (March 21, 2017). https://jamestown.org/program/russian-national-guard-new-oprichnina-cyber-police-something-else-2/.

"Swiss Police 'Exposed Russian Spies in Davos'," *BBC*, January 21, 2020, https://www.bbc.com/news/world-europe-51196659.

Szabolcs, Panyi. "Russian Diplomats Caught Spying in Hungary Get Expelled Quietly As Usual." Direkt36 (Hungary), December 20, 2018. https://www.direkt36.hu/en/orosz-diplomatakat-ertek-kemkedesen-magyarorszagon-es-szep-csendben-ki-is-szoritottak-oket/.

Taylor, Adam. "The Recent History of Terrorist Attacks in Russia." *Washington Post*, April 3, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/04/03/the-recent-history-of-terrorist-attacks-in-russia/.

"Timeline: The Beslan School Siege." *Guardian*, September 6, 2004, https://www.theguardian.com/world/2004/sep/06/schoolsworldwide.chechnya.

Tóda, Mirek. "A Russian Spy's Manual: Send a Secret Message to the Strela-3 Satellite and Betray NATO Allies." *Dennik N*, October 11, 2020, https://dennikn.sk/2082755/russian-spys-manual-send-a-secret-message-to-the-strela-3-satellite-and-betray-nato-allies/.

Trevithick, Joseph. "Russia's Electronic Spies Are Hard at Work in Syria: Signal Spooks Search for Targets and Follow Up on Strikes." Warisboring.com, October 7, 2015, https://warisboring.com/russias-electronic-spies-are-hard-at-work-in-syria/.

Troianovski, Anton, Ellen Nakashima, and Shane Harris. "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West." *Washington Post*, December 28, 2018, https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

Tucker, Emma. "Swiss Police Suspect Russian Spies Posed as Plumbers to Surveil Davos: Report." *Daily Beast*, January 21, 2020, https://www.thedailybeast.com/swiss-police-suspect-russian-spies-posed-as-plumbers-to-surveil-davos-report-says.

Tucker, Patrick. "Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says." *Defense One*, December 7, 2018, https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/.

"U.S. Hits Russian Oligarchs and Officials With Sanctions Over Election Interference." *NPR*, April 6, 2018, https://www.npr.org/sections/thetwo-way/2018/04/06/600083466/u-s-hits-russian-oligarchs-and-officials-with-sanctions-over-election-interferen.

"US Provided Information on Terrorist Plotters in Russia, Says FSB chief." *TASS*, October 17, 2019, https://tass.com/politics/1083742.

"Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units." *CrowdStrike*, March 23, 2017, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

"'V' for 'Vympel: FSB's Secretive Department 'V' Behind Assassination of Georgian Asylum Seeker In Germany." *Bellingcat*, February 17, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/.

Vanin, Vladimir. “Ай да мы: взяли русского Джеймса Бонда!” [“Oh My: A Russian James Bond Is Arrested!”]. *Nezavisimoe Voennoe Obozrenie*, January 22, 2010.

Vaux, Pierre. “Fontanka Investigates Russian Mercenaries Dying for Putin in Syria and Ukraine.” *The Interpreter*, March 29, 2016, https://www.interpretermag.com/fontanka-investigates-russian-mercenaries-dying-for-putin-in-syria-and-ukraine/.

Vetrova, Olga. “Росгвардия усмотрела схожесть протестов в РФ с ‘цветными’ революциями” [“The Russian National Guard Sees a Similarity Between Protests in the RF and ‘Color’ Revolutions”]. *New Day*, June 16, 2017, https://newdaynews.ru/moskow/606096.html.

Vinogradov, Egor. “Движение ‘За честные выборы’ начало новую серию протестов” [“The ‘For Honest Elections’ Movement Began a New Series of Protests”]. *Deutsche Welle* (in Russian), March 6, 2012.

Wakefield, Jane. “Russia ‘Successfully Tests’ Its Unplugged Internet.” *BBC*, December 24, 2019, https://www.bbc.com/news/technology-50902496.

Walsh, Nick Paton. “Russia Says ‘Spies’ Work in Foreign NGOs,” *Guardian*, May 13, 2005, https://www.theguardian.com/world/2005/may/13/russia.nickpatonwalsh.

Watkins, Ali. “Russia Escalates Spy Games After Years of U.S. Neglect.” *Politico*, June 1, 2017, https://www.politico.com/story/2017/06/01/russia-spies-espionage-trump-239003.

Watkins, Steffan. “We Will Bury You (in Data)—Russian Navy Yantar Backgrounder and Summer 2016 Trip Report.” vesselofinterst.com, November 3, 2018, https://www.vesselofinterest.com/2018/11/we-will-bury-you-in-data-russian-navy.html.

“Were Top FSB Officials Jailed over Oligarchs’ Struggle?” *Warsaw Institute*, April 27, 2019, https://warsawinstitute.org/top-fsb-officials-jailed-oligarchs-struggle/.

Whittaker, Zack. “Bellingcat Journalists Targeted by Failed Phishing Attempt.” *Tech Crunch*, July 27, 2019, https://techcrunch.com/2019/07/27/bellingcat-targeted-failed-phishing-attempt/.

“Who’s Asking? ‘Yandex’ Releases First-ever Transparency Report on Requests for User Data From the Russian authorities.” *Meduza*, October 26, 2020, https://meduza.io/en/feature/2020/10/26/who-s-asking.

Williams, Matthias. “Russian Diplomats Expelled From Moldova Recruited Fighters—Sources.” Reuters, June 13, 2017, https://www.reuters.com/article/us-moldova-russia-expulsions/exclusive-russian-diplomats-expelled-from-moldova-recruited-fighters-sources-idUSKBN1941DA.

Williams, Pete. “Russian Hackers Targeted Control Systems for Electric Utilities, Homeland Security Says.” *NBC News*, July 24, 2018, https://www.nbcnews.com/politics/politics-news/russian-hackers-targeted-control-systems-electric-utilities-homeland-security-says-n894226.

Windrem, Robert. “Timeline: Ten Years of Russian Cyber Attacks on Other Nations.” *NBC News*, December 18, 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

World Anti-Doping Agency. "WADA Confirms Attack by Russian Cyber Espionage Group." Press Release, September 13, 2016, https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group.

Yaffa, Joshua. "How Bill Browder Became Russia's Most Wanted Man." *The Atlantic*, August 13, 2018, https://www.newyorker.com/magazine/2018/08/20/how-bill-browder-became-russias-most-wanted-man.

"Yarovaya Law Obliges Operators and Internet Companies To Store User Correspondence." *TASS*. July 1, 2018, https://tass.com/politics/1011585.

Zagorin, Adam. "Still Spying After All These Years." *Time*, June 29, 1992.

Zak, Anatoliy. "Araks (11F664) Military Spacecraft." *RussianSpaceWeb*, January 3, 2018, http://www.russianspaceweb.com/araks.html.

Zak, Anatoliy. "Bars-M: Russia's First Digital Cartographer." *RussianSpaceWeb*, last updated February 5, 2020, http://www.russianspaceweb.com/bars-m.html.

Zak, Anatoliy. "The EKS Kupol Network Design." *RussianSpaceWeb*, last updated December 28, 2019, http://www.russianspaceweb.com/eks-network.html.

Zak, Anatoliy. "Lotos-S Spacecraft for the Liana System." *RussianSpaceWeb*, October 25, 2018, http://www.russianspaceweb.com/images/spacecraft/military/elint/liana/lotos_m_silo_1.jpg.

Zak, Anatoliy. "Origin of the Vostochny (formerly Svobodny) Launch Site." *Russian Space Web*, September 8, 2018, http://www.russianspaceweb.com/svobodny.html.

Zak, Anatoliy. "Persona (14F137) Spy Satellite." *RussianSpaceWeb*, August 29, 2017, http://www.russianspaceweb.com/persona.html.

Zak, Anatoliy. "US-A and US-P military satellites." *RussianSpaceWeb*, last updated January 2, 2020, http://www.russianspaceweb.com/us.html.

Zak, Anatoliy. "US-K and US-KMO constellations," *RussianSpaceWeb*, last updated November 25, 2019, http://www.russianspaceweb.com/oko.html.

Żemła, Edyta. "Piotr Ś. mógł przekazać Rosji plany NATO-wskiej dywizji w Polsce" ["Piotr Ś. Could Provide Russia the Plans for a NATO Division in Poland"]. *Onet News*, November 2, 2019, https://wiadomosci.onet.pl/kraj/piotr-s-mogl-przekazac-rosji-plany-nato-wskiej-dywizji-w-polsce/q0dxdyn.

Russian Titles (Government Documents and Journalism Articles)

"В МИД России пожаловались на 'план Даллеса'" ["Complaints About the 'Dulles Plan' at the MFA"]. Lenta.ru, May 14, 2020. https://lenta.ru/news/2020/05/14/dalles/.

"Глава СВР Нарышкин подтвердил, что в советские времена работал в Брюсселе" ["SVR Chief Confirmed that During the Soviet Times He Worked in Brussels"]. *RIA Novosti,* September 5, 2020. https://ria.ru/20200905/naryshkin-1576816627.html.

"Да здравствует ВЧК-ОГПУ, верный и могущественный страж пролетарской диктатуры" ["Long Live the VChK-OGPU, the Faithful and Powerful Protector of the Proletarian Dictatorship"]. *Pravda*, December 18, 1927.

"Дело Советских Шпионов в Латвии" ["The Case of Soviet Spies in Latvia"]. *Vozrozhdenie*, July 24, 1928.

"Заседание коллегии Федеральной службы безопасности" ["Conference of the Federal Security Service Collegium"]. Kremlin.ru, February 14, 2013. http://*kremlin.ru*/events/president/news/17516.

"Заседание коллегии Федеральной службы безопасности" ["Conference of the Federal Security Service Collegium"]. Sosluzhivtsi.ru, February 26, 2016. https://sosluzhivtsi.ru/public/politika/1977-zasedanie-kollegii-fsb/.

"Заседание коллегии Федеральной службы безопасности" ["Conference of the Federal Security Service Collegium"]. Kremlin.ru, February 16, 2017. http://kremlin.ru/events/president/news/53883.

"Заседание коллегии Федеральной службы безопасности" ["Conference of the Federal Security Service Collegium"]. Kremlin.ru, March 5, 2018. http://kremlin.ru/events/president/news/56977.

"Заседание коллегии Федеральной службы безопасности" ["Conference of the Federal Security Service Collegium"]. Kremlin.ru, March 6, 2019. http://kremlin.ru/events/president/news/59978.

"Заседание коллегии ФСБ" ["Conference of the FSB Collegium"]. Kremlin.ru, February 20, 2020. http://kremlin.ru/events/president/news/62834.

"Заседание коллегии ФСБ России" ["Conference of the FSB Collegium of Russia"]. Kremlin.ru, February 24, 2021. http://www.kremlin.ru/events/president/news/65068.

"Лубянская Федерация: Как ФСБ определяет политику и экономику России" ["The Lubyanka Federation: How the FSB Determines the Politics and Economics of Russia"]. *Dossier Center*, 2020. https://fsb.dossier.center/.

"Матвиенко назвала задержание Бочкарева в Норвегии провокацией" ["Matvienko Called Bochkarev's Arrest in Norway a Provocation"]. *RIA Novosti*, October 22, 2018.

"Новый глава ФСО Кочнев служит в органах госохраны 14 лет" ["New FSO Chief Kochnev Has Served in the State Protection Organs for 14 Years"]. *TASS*, May 26, 2016. https://tass.ru/politika/3317285.

"Объединенная двигателестроительная корпорация подтвердила задержание своего сотрудника" ["United Engine Corporation Confirms the Arrest of Its Employee"]. *Interfax*, September 5, 2019.

"'Окно' в Таджикистане 'увидит' объекты в космосе на расстоянии 50 тысяч км" [The "'Okno' in Tajikistan 'Sees' Objects in Space at a Distance of 50 Thousand km"]. *RIA Novosti*, November 27, 2016. https://news.rambler.ru/science/35393642-okno-v-tadzhikistane-uvidit-obekty-v-kosmose-na-rasstoyanii-50-tysyach-km/.

“Опрос показал, хотят ли россияне карьеры разведчика для своих детей” [“Survey Shows Whether Russians Want an Intelligence Officer Career for Their Children”]. *RIA Novosti*, November 5, 2019. https://ria.ru/20191105/1560570969.html.

Подвиг Разведчика [*The Intelligence Officer’s Deed*], 1947, released in 1949 in the United States as *Secret Agent*. https://www.imdb.com/title/tt0039716/.

“Путин рассказал, что его работа в КГБ была связана с нелегальной разведкой” [“Putin Related that His Work in the KGB Was Connected to Illegal Intelligence”]. *RIA Novosti*, June 6, 2017. https://ria.ru/20170624/1497218985.html?in=t.

Разведчики Разоблачают... Эта Кинга о Шпионской и Подрывной Деятельности Радиостанций “Свобода” и “Свободная Европа” [*Intelligence Officers Reveal... This Book Is About the Espionage and Underground Activity of the Radio Stations “Liberty” and “Free Europe”*]. Moscow: Molodaya Gvardiya, 1977.

“Рогозин опубликовал фото с бойцами ‘Заслона’ в Сирии” [“Rogozin Published a Photo with ‘Zaslon’ Soldiers in Syria”]. *Vzglyad*, May 24, 2014. https://vz.ru/news/2014/5/24/688286.html.

“Российской контрразведке исполнилось 80 лет” [“Russian Counterintelligence Has Turned 80 Years Old”]. *RIA Novosti*, May 5, 2002, https://ria.ru/20020506/135030.html.

Семнадцать Мгновений Весны [*Seventeen Moments of Spring*], 1973. https://www.imdb.com/title/tt0069628/.

“Семья шпиона Смоленкова сбежала из своего дома в США” [“The Family of Spy Smolenkov Have Disappeared from Their Home in the USA”]. Lenta.ru, September 11, 2019, https://lenta.ru/news/2019/09/11/runaway/.

“Сергей Нарышкин: нелегалы—золотой фонд внешней разведки” [“Sergey Naryshkin: Illegals Are the Golden Reserve of Foreign Intelligence”]. *TASS*, June 27, 2017, https://tass.ru/interviews/4366965.

“Спецназ СВР” [“SVR Spetsnaz”]. Agentura.ru. http://www.agentura.ru/dossier/russia/svr/specnaz/.

“Торжественное мероприятие по случаю 100-летия ГРУ” [“Celebration for the 100th Anniversary of the GRU”]. Kremlin.ru, November 2, 2018. http://kremlin.ru/events/president.news/59032.

“Увидеть футбольный мяч с 8000 км: как устроена ПВО России” [“To See a Football from 8,000 km: That Is How the PVO of Russia Works”]. *TVZvezda*, May 17, 2015.

“ФСБ, ГРУ, ФСО, СВР... не боги” [“The FSB, GRU, FSO, SVR...Are Not Gods”]. Glagolurfo.com, December 16, 2020. http://glagolurfo.com/newsitems/2020/12/16/fsb-gru-fso-svr-ne-bogi/.

“ФСБ сюсюкать не будет: На все угрозы национальной безопасности Путин пообещал адекватный ответ” [“The FSB Is Not Lisping: Putin Promised an Active Response to All Threats to National Security”]. Lenta.ru, March 26, 2015.

“ФСО” [“FSO”], *Voenpro*, October 22, 2013. https://voenpro.ru/infolenta/fco.

"'Штучные люди': СВР рассекретила выдающихся разведчиков-нелегалов" ["'Extraordinary People': The SVR Declassified Outstanding Illegal Intelligence Officers"]. *RIA Novosti*, January 28, 2020. https://ria.ru/20200128/1563982674.html.

"'Яндекс' подтвердил наличие решения по ключам шифрования для ФСБ" ["Yandex Confirmed Having Reached a Solution to Encryption Keys for the FSB"]. *RBC*, June 7, 2019. https://www.rbc.ru/society/07/06/2019/5cfa2a169a7947affada5b1a.

ENDNOTES

[1] Russian SVR Archives, Operational Record File No. 76659, vol. 1, 245–58, quoted in John Costello and Oleg Tsarev, *Deadly Illusions: The KGB Orlov Dossier Reveals Stalin's Master Spy* (New York: Crown, 1993), 308–12.

[2] Alexander Orlov, *The Secret History of Stalin's Crimes* (New York: Random House, 1953).

[3] Alexander Orlov, *Handbook of Intelligence and Guerrilla Warfare* (Ann Arbor: University of Michigan Press, 1963).

[4] Federal Bureau of Investigation (FBI), "Comments of Alexander Orlov about Walter Krivitsky's Book *In Stalin's Secret Service*," FBI Memo, October 13, 1954, The National Archives, Kew London, UK, KV 2/2879, serial 45b, 10-12.

[5] Alexander Orlov, "The Theory and Practice of Soviet Intelligence," *Studies in Intelligence* 7, no. 1 (Spring 1963): 45.

[6] For a description of this equation as it is applied to foreign intelligence activities, see Kevin P. Riehle, "Assessing Foreign Intelligence Threats," *American Intelligence Journal* 31, no. 1 (2013): 96-101, https://www.jstor.org/stable/26202049.

[7] Ben B. Fischer, ed., *Okhrana: The Paris Operations of the Russian Imperial Police* (Washington, DC: CIA Center for the Study of Intelligence, 1997).

[8] Esther B. Fein, "Soviets Confirm Nazi Pacts Dividing Europe," *New York Times*, August 19, 1989, https://www.nytimes.com/1989/08/19/world/soviets-confirm-nazi-pacts-dividing-europe.html.

[9] Aleksandr Yakovlev Database, https://www.alexanderyakovlev.org/db-docs.

[10] See, for example, A. M. Plekhanov and A. A. Plekhanov, *Ф.Э. Дзержинский—Председатель ВЧК—ОГПУ. 1917–1926* [*F. E. Dzerzhinskiy—Chief of the VChK-OGPU 1917-1926*] (Moscow: International Democracy Foundation, 2007); V. N. Khaustov, V. P. Naumov, and N. S. Plotnikova, *Лубянка. Сталин и МГБ. Март 1946 – март 1953: Документы*

высших органов партийной и государственной власти [*Lubyanka. Stalin and the MGB, March 1946 – March 1953: Documents of the Higher Organs of Party and State Power*] (Moscow: International Democracy Foundation, 2007); V. A. Gavrilov, *Военная Разведка Информирует: Документы Разведуправления Красной Армии. Январь 1939 – июнь 1941 г.* [*Military Intelligence Informs: Documents from the Red Army Intelligence Directorate, January 1939 – June 1941*] (Moscow: International Democracy Foundation, 2008); N. V. Petrov and Ya. Foytsik, *Аппарат НКВД-МГБ в Германии. 1945–1953* [*The NKVD-MGB Apparatus in Germany, 1945-1953*] (Moscow: International Democracy Foundation, 2009).

[11] Alexander Vassiliev Notebooks, Wilson Center Digital Archive, https://digitalarchive.wilsoncenter.org/collection/86/vassiliev-notebooks.

[12] Allen Weinstein and Alexander Vassiliev, *The Haunted Wood* (New York: Modern Library, 2000); John Earl Haynes, Harvey Klehr, and Alexander Vassiliev, *Spies: The Rise and Fall of the KGB in America* (New Haven: Yale University Press, 2010).

[13] Costello and Tsarev, *Deadly Illusions*.

[14] Nigel West and Oleg Tsarev, *The Crown Jewels: The British Secrets at the Heart of the KGB Archives* (New Haven: Yale University Press, 1999).

[15] Philip Knightley, "Disinformation," *London Review of Books*, July 8, 1993, https://www.lrb.co.uk/the-paper/v15/n13/phillip-knightley/disinformation; see also Andrei Soldatov and Irina Borogan, *The Compatriots: The Brutal and Chaotic History of Russia's Exiles, Émigrés, and Agents Abroad* (New York: Public Affairs, 2019), 161-67.

[16] Yevgeniy Primakov, ed., *Очерки Истории Российской Внешней Разведки* [*Essays on the History of Russian Foreign Intelligence*], six volumes, (Moscow: Mezhdunarodniya Otnosheniya, 1997-2006).

[17] Sergey A. Korenkov, ed., *Военная Контрразведка ФСБ России 1918–2003* [*Military Counterintelligence of the FSB of Russia, 1918–2003*] (Moscow: Moskovskiy Poligraficheskiy Dom, 2004).

[18] V. Vinogradov, A. Litvin, and V. Khristoforov, eds., *Архив ВЧК: Сборник документов* [*The VChK Archive: A Collection of Documents*] (Moscow: Kukovo Pole, 2007).

[19] Vladimir Dolmatov, ed., *Служба Внешней Разведки Российской Федерации 100 Лет: Документы и Свидетельства* [*The Foreign Intelligence Service of the Russian Federation at 100 Years: Documents and Testimonies*] (Moscow: Komsomolskaya Pravda, 2020); see also A. A. Zdanovich and A. G. Bezverkhniy, eds., *Труды Общества Изучения Истории Отечественных Спецслужб* [*Works of the Society for Studying the History of Domestic Special Services*], three volumes (Moscow: Kuchkove Pole, 2006 and 2007).

[20] KGB Documents Online, https://www.kgbdocuments.eu/kgb-journals-and-books/.

[21] Dmitriy Prokhorov, *Сколько стоит продать Родину?* [*What is the Cost of Betraying One's Homeland?*] (Moscow: OLMA-Press, 2005).

[22] Vitaliy Karavashkin, *Кто Предал Россию* [*Who Betrayed Russia*] (Moscow: AST, 2008).

23 See Filip Kovacevic, "Nikolay Dolgopolov: The Storyteller of Soviet Intelligence History," *Intelligence and National Security*, published online August 13, 2020, https://www.tandfonline.com/doi/abs/10.1080/02684527.2020.1805167.

24 Pavel Sudoplatov, *Special Tasks: The Memoirs of an Unwanted Witness—A Soviet Spymaster* (Boston: Little, Brown and Company, 1994).

25 Pavel Sudoplatov, *Спецоперации. Лубянка и Кремль 1930–1950 годы* [*Special Operations: Lubyanka and the Kremlin, 1930-1950*] (Moscow: OLMA-Press, 1997).

26 See, for example, Oleg Kalugin, *Spymaster: My Thirty-two Years in Intelligence and Espionage Against the West* (New York: Basic Books, 2009); Victor Cherkashin, *Spy Handler: Memoir of a KGB Officer. The True Story of The Man Who Recruited Robert Hanssen & Aldrich Ames* (New York: Basic Books, 2004); Yuriy Drozdov, *Записки начальника нелегальной разведки* [*Notes of a Chief of Illegal Intelligence*] (Moscow: Russian Biographical Institute, 1999); Andrey Bronnikov and Yelena Vavilova, *Женщина, которая умеет хранить тайны* [*The Woman Who Knows How to Keep Secrets*] (Moscow, Eksmo, 2019).

27 Robert Legvold, "Review of *Special Tasks: The Memoirs of an Unwanted Witness, A Soviet Spymaster,* by Pavel Sudoplatov and Anatoli Sudoplatov with Jerrold Schechter," *Foreign Affairs,* July/August 1994, https://www.foreignaffairs.com/reviews/capsule-review/1994-07-01/special-tasks-memoirs-unwanted-witness-soviet-spymaster.

28 See, in particular, U.S. National Archives and Records Administration, Records of the Central Intelligence Agency (Record Group 263); U.S. Army Staff, Investigative Records Repository (Record Group 319).

29 See, for example, David Murphy, Sergei Kondrashev, and George Bailey, *Battleground Berlin: CIA vs. KGB in the Cold War* (New Haven: Yale University Press, 1997); Cees Wiebes and Przemysław Gasztold, "Polish Intelligence in the Netherlands and Dutch Counter-Intelligence, 1947-1962," *International Journal of Intelligence, Security, and Public Affairs*, published online November 3, 2020, https://www.tandfonline.com/doi/abs/10.1080/23800992.2020.1839726?journalCode=usip20.

30 "Ottawa Denies Soviet Spy Defected Here," *The Gazette* (Montreal), March 27, 1972, 3.

31 Gordon Corera, *Russians Among Us: Sleeper Cells, Ghost Stories, and the Hunt for Putin's Spies* (New York: William Morrow, 2020).

32 National Security Agency, *Venona*, https://www.nsa.gov/news-features/declassified-documents/venona/.

33 See Kevin Riehle, *Soviet Defectors: Revelations of Renegade Intelligence Officers, 1924-1954* (Edinburgh: Edinburgh University Press, 2020).

34 Russian Federation, Указ Президента Российской Федерации от 22.10.2007 No. 1404, "О Присвоении Звания Героя Российской Федерации Ковалю Ж.А." [Order of the President of the Russian Federation No. 1404, October 22, 2007, "Awarding the Rank of Hero of the Russian Federation to Koval Zh. A."], https://rulaws.ru/president/Ukaz-Prezidenta-RF-ot-22.10.2007-N-1404/; see also Michael Walsh, "George Koval: Atomic

Spy Unmasked," *Smithsonian Magazine*, May 2009, https://www.smithsonianmag.com/history/george-koval-atomic-spy-unmasked-125046223/.

35 For the website of Russia's Federal Security Service (FSB), see www.fsb.ru; for the website of Russia's Foreign Intelligence Service (SVR), see www.svr.gov.ru.

36 Fischer, ed., *Okhrana*, p. 6, n10.

37 Vladimir Putin, "Поздравление с Днём работника органов безопасности" ["Congratulations on Security Service Workers' Day"], Kremlin.ru, December 20, 2020, http://www.kremlin.ru/events/president/news/64681.

38 Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), 24.

39 Fedor Pavlovich Drugov, "С Дзержинским в ВЧК: Исповедь раскаявшегося чекиста" ["With Dzerzhinskiy in the VChK: The Confession of a Repentant Chekist"], *Illustrated Russia*, February 7, 1931, 1.

40 Viktor Mikhailovich Chebrikov, ed., *История Советских Органов Государственной Безопасности: Учебник* [*The History of Soviet State Security Agencies: A Textbook*] (Moscow: Dzerzhinskiy Higher Red Banner School of the Committee of State Security, 1977), 8.

41 Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (New York: Harper-Collins Publishers, 1990), 22; Oleg Danilovich Kalugin, *Вид с Лубянки: "Дело" бывшего генерала КГБ* [*The View from Lubyanka: The "Case" of a Former KGB General*] (Moscow: PIK, 1990) (online publication).

42 Fischer, ed., *Okhrana*.

43 Chebrikov, ed., *The History of Soviet State Security Agencies*, 14.

44 Fischer, ed., *Okhrana*, 36-38.

45 Andrew and Mitrokhin, *The Sword and the Shield*, 25-26.

46 Andrew and Mitrokhin, *The Sword and the Shield*, 41.

47 Sudoplatov, *Special Tasks*, 91.

48 British Home Office Warrant, July 25,1930, The National Archives, Kew, London, KV 3/2398, serial 12a.

49 Korenkov, ed., *Military Counterintelligence of the FSB*, 1.

50 Harvard Project on the Soviet Social System. Schedule A, Vol. 11, Case 144 (interviewers A.P., and R.B., type A4), 24-25.

51 See, for example, Andrew and Mitrokhin, *The Sword and the Shield*, 314.

52 Fischer, ed., *Okhrana*, 77-78.

53 Peter Pavlonovsky (aka Sumarokov), biography submitted as a statement in his trial in July 1929, Hoover Institution Archive, Boris Nicolaevsky Collection, Box 217, Folder 6 (Microfilm 187).

54 Richard B. Spence, "Senator William E. Borah: Target of Soviet and Anti-Soviet Intrigue, 1922–1929," *International Journal of Intelligence and CounterIntelligence* 19, no. 1 (2006): 134-55.

55 Prokhorov, *What is the Cost of Betraying One's Homeland?,* 28.

56 Spence, "Senator William E. Borah," 135.

57 Vasili Mitrokhin, ed., *KGB Lexicon: The Soviet Intelligence Officer's Handbook* (London: Frank Cass, 2002), 13.

58 Thomas Rid, *Active Measures: The Soviet History of Disinformation ad Political Warfare* (New York: Farrar, Strauss, and Giroux, 2020), 123-41, 201-02, 206-08, 313.

59 Rid, *Active Measures*, 210.

60 Fischer, ed., *Okhrana*, 8.

61 V. I. Savalyev, "*Многоликость Разведки*" ["The Many Faces of Intelligence"], in Yevgeniy Primakov, ed., *Очерки Истории Русской Внешней Разведки* (*Essays on the History of Russian Foreign Intelligence*), Vol. 1, (Moscow: Mezhdunarodniye Otnosheniya, 1996), 212-13.

62 S. M. Golubev, "Операция 'Трест'" ["Operation 'Trust'"], in Yevgeniy Primakov, ed., *Очерки Истории Российской Внешней Разведки* [*Essays on the History of Russian Foreign Intelligence*], vol. 2 (Moscow: Mezdunarodnye Otnosheniya, 1997), 111-28.

63 Vladimir Burtsev, "Police Provocation in Russia," *The Slavonic Review* 6, no. 17 (December 1927): 247-67, https://www.jstor.org/stable/4202167?seq=1.

64 John Dziak, *Chekisty: A History of the KGB* (Lexington, MA: Lexington Books, 1988).

65 Foreign Intelligence Service of the Russian Federation, "20 Декабря 1920 года" ("20 December 1920"), http://svr.gov.ru/calendar/6191.htm.

66 "Российской контрразведке исполнилось 80 лет" ["Russian Counterintelligence Has Turned 80 Years Old"], *RIA Novosti*, May 5, 2002, https://ria.ru/20020506/135030.html.

67 Georgiy Agabekov, *ЧК за работой* [*The Cheka at Work*] (Berlin: Strela, 1931), 62-63.

68 Agabekov, *The ChK at Work*, 50-54; Georgiy Agabekov, *OGPU: The Russian Secret Terror,* trans. Henry W. Bunn (New York: Brentano's, 1931), 35-36, 44.

69 Peter Hopkirk, *Setting the East Ablaze: Lenin's Dream of an Empire in Asia* (New York: Kodansha International, 1984).

70 Calculation based on "... in 1917, 100 rubles would buy $9" (Egorova and Zubachevya) and U.S. dollar inflation since 1917 (Dollar Times): Kira Egorova and Ksenia Zubacheva, "The Ruble's Journey Through Time, from the Middle Ages to the Present Day," *Russia Beyond*, May 14, 2020; https://www.rbth.com/business/332176-history-russian-rubl; "Calculate the Value of $1.00 in 1917: What Is $1 in 1917 Worth in Today's Money?," Dollar Times, accessed on March 11, 2021, https://www.dollartimes.com/inflation/inflation.php?amount=1&year=1917.

71 David W. McFadden, *Alternative Paths: Soviets and Americans, 1917-1920* (Oxford: Oxford University Press, 1993), 19-21.

72 Lev Davydovich Trotsky, *Моя Жизнь* [*My Life*], vol. 2 (Berlin, Granit, 1930), 62-64.

73 The Comintern, also known as the Third International, was an international association of communist parties. For a discussion of Moscow's control over the Comintern, see David W. Lovell and Kevin Windle, eds., "Piecing Together the Past: The Comintern, the CPA, and

the Archives," in *Our Unswerving Loyalty: A Documentary Survey of Relations between the Communist Party of Australia and Moscow, 1920-1940* (Canberra: ANU Press, 2008), 1–17.

74 See, for example, Petr Karpov, *Организация ГПУ* [*The Organization of the GPU*], undated typescript, Hoover Institution Archives, Boris Nicolaevsky Collection, Box 217, Folder 6 (Microfilm reel 187); Report by Yevgeniy Kozhevnikov titled "Work of the Representatives of the 'U.S.S.R.' in China," forwarded by Shelley to the War Office on June 20, 1927, The National Archives, Kew, London, KV 2/1895, serial 15b; "Дело Советских Шпионов в Латвии" ["The Case of Soviet Spies in Latvia"], *Vozrozhdenie*, July 24, 1928; Andrey Pavlovich Smirnov, "Записки агента Разведупра" ["Notes of a Razvedupr Agent"], *Vozrozhdenie*, March 28, 1930, 3; MI5, Compilation of Ginzberg's MI5 debriefings, "Information Obtained from General Krivitsky During His Visit to This Country, January-February 1940," The National Archives, KV 2/805, serial 55x.

75 Georgiy Agabekov, *Секретный Террор* [*Secret Terror*] (Moscow: Terra, 1998).

76 F. E. Dzerzhinskiy to I. S. Unshlikht, Telegram dated September 5, 1922, Alexander Yakovlev Archive, http://www.alexanderyakovlev.org/fond/issues-doc/1019506.

77 Alastair Kocho-Williams, *Engaging the World: Soviet Diplomacy and Foreign Propaganda in the 1920s*, University of the West of England, December 2007, https://www2.uwe.ac.uk/faculties/CAHE/HPP/staff/stafflist/A_Kocho-Williams_sovietdiplomats1920s.pdf.

78 Quoted in David W. McFadden, "After the Colby Note: The Wilson Administration and the Bolsheviks, 1920-21," *Presidential Studies Quarterly* 25, no. 4 (Fall 1995): 741-50.

79 McFadden, *Alternative Paths*, 19.

80 U.S. Embassy Havana to Department of State, Despatch 1437, May 25, 1926, National Archives and Records Administration, RG 59, Central Decimal File 1910-1929, Box 7330, Serial 811.00B/585; see also Mikhail Hendler letter to Congressman Hamilton Fish, dated November 23, 1930, Richard J. O'Melia Collection, Hesburgh Libraries, University of Notre Dame, Correspondence Box XVI, item 55.

81 Christopher Andrew, *The Defence of the Realm: The Authorized History of MI5* (London: Allen Lane, 2009), 154.

82 MI5, Compilation of Ginzberg's MI5 debriefings. "Information Obtained from General Krivitsky."

83 British Embassy Washington Memo, September 13, 1940, The National Archives, Kew, London, FO 371/24845, 2.

84 Kevin Riehle, "Soviet Intent at the Dawn of the Cold War: Igor Gouzenko's Revelations about GRU Intelligence Taskings," *Journal of Intelligence History*, February 25, 2021, https://www.tandfonline.com/doi/abs/10.1080/16161262.2021.1892997?journalCode=rjih20.

85 See, for example, Barton Whaley, *Soviet Clandestine Communication Nets: Notes for a History of the Structures of the Intelligence Services of the USSR* (Cambridge, MA: MIT Center for International Studies, 1969), 1; Evgenia Lezina, "Dismantling the State Security Apparatus Transformations of the Soviet State Security Bodies in Post-Soviet Russia," in Nikolai Bobrinsky et

al., *Memory of Nations: Democratic Transition Guide: the Russian Experience* (Prague: CEVRO, 2017), 7; Thomas Polgar, *The KGB: An Instrument of Soviet Power* (McLean, VA: Association of Former Intelligence Officers, 1989), 8; Richard Sakwa, *Russian Politics and Society* (London: Routledge, 2002), 91; Kathryn S. Olmsted, *Red Spy Queen: A Biography of Elizabeth Bentley* (Chapel Hill, NC: University of North Carolina Press, 2002), 210.

86 "Да здравствует ВЧК-ОГПУ, верный и могущественный страж пролетарской диктатуры" ["Long Live the VChK-OGPU, the Faithful and Powerful Guardian of the Proletarian Dictatorship"], *Pravda*, December 18, 1927, 3.

87 Mondich's book was first published in Russian under the pen name N. Sinevirskiy, *СМЕРШ: Год в Стане Врага* [*SMERSH: A Year in the Enemy's Camp*] (Limburg an der Lahn, Germany: Possev, 1948). It was published in English as Nicola Sinevirsky, *SMERSH* (New York: Henry Holt, 1950).

88 Ian Fleming, *From Russia with Love* (London: Penguin, 1957), 6.

89 Korenkov, ed., *Military Counterintelligence of the FSB*.

90 Australian Security Intelligence Organisation Report, "The Committee of Information ('KI'), 1947–1951," November 17, 1954, National Archives of Australia, A6283, folder 16, item number4104677, 1.

91 See also Andrew and Mitrokhin, *The Sword and the Shield*, 144-46.

92 Murphy, Kondrashev, and Bailey, *Battleground Berlin*, 28-29.

93 As quoted in David J. Dallin, *Soviet Espionage* (New Haven: Yale University Press, 1955), viii.

94 Kevin Riehle, "The Defector Balance Sheet: Westbound Versus Eastbound Intelligence Defectors from 1945 to 1965," *International Journal of Intelligence and Counterintelligence* 33, no. 1 (2020): 68-96, https://www.tandfonline.com/doi/abs/10.1080/08850607.2019.1670021?journalCode=ujic20.

95 *Подвиг Разведчика* [*The Intelligence Officer's Deed*], 1947, released in 1949 in the United States as *Secret Agent*, https://www.imdb.com/title/tt0039716/. Some historians assert that the prototype for the hero in this movie was not Khokhlov but Nikolay Kuznetsov, a Soviet illegal intelligence officer who penetrated the German government during World War II and who is now portrayed in heroic terms in Russian historical narratives; see, for example, Viktoriya Sukovata, "Evolution of Trauma: Memories of War in Russian Spy Cinema," *Baltic Worlds* 2, no. 2 (2019): 29-36; also email correspondence from Dr. Filip Kovacevic, University of San Francisco, January 12, 2021.

96 Tennant Bagley, *Spymaster: Startling Cold War Revelations of a Soviet KGB Chief* (New York: Skyhorse Publishing, 2013), 153-64; Henry Sakaida and Christa Hook, *Heroes of the Soviet Union 1941–45* (Oxford: Osprey Publishing, 2004), 32.

97 *Семнадцать Мгновений Весны*, 1973 [*Seventeen Moments of Spring*], https://www.imdb.com/title/tt0069628/; see also Isabelle de Keghel, "Seventeen Moments of Spring, a Soviet James Bond Series? Official Discourse, Folklore, and Cold War Culture in Late Socialism,"

Euxeinos 8, no. 25-26 (2018): 82-93; Catharine Theimer Nepomnyashchy, "The Blockbuster Miniseries on Soviet TV: Isaev-Shtirlits, the Ambiguous Hero of *Seventeen Moments of Spring*," *The Soviet and Post-Soviet Review*, no. 29 (2002): 257-76; Jeremy Dwyer, "Masculinities and Anxieties in the Post-Soviet Boevik Novel," *Australian Slavonic and Eastern European Studies Journal* 22, no. 1-2 (2008): 1-21; Erik Jens, "Cold War Spy Fiction in Russian Popular Culture: From Suspicion to Acceptance via *Seventeen Moments of Spring*," *Studies in Intelligence* 62, no. 2 (June 2017): 31-41.

98 Jeff Trimble, "Spreading The Word: The KGB's Image-Building Under Gorbachev," Discussion Paper D-24, The Joan Shorenstein Center, John F. Kennedy School of Government, Harvard University, February 1997.

99 Lezina, "Dismantling the State Security Apparatus," 9.

100 "Торжественное мероприятие по случаю 100-летия ГРУ" ["Celebration for the 100th Anniversary of the GRU"], Kremlin.ru, November 2, 2018, http://kremlin.ru/events/president.news/59032.

101 MI5, Compilation of Ginzberg's MI5 debriefings. "Information Obtained from General Krivitsky," 2.

102 Elizabeth Poretsky, *Our Own People* (Ann Arbor: University of Michigan University Press, 1969), 2.

103 MI5, Compilation of Ginzberg's MI5 debriefings. "Information Obtained from General Krivitsky."

104 Alexander Barmine, *Memoirs of a Soviet Diplomat* (London: Lovat Dickson, 1938), ix-x.

105 Aleksandr Salikhov, "От Региступра до ГРУ: путь длиной в 88 лет" ["From Registupr to GRU: The 88-year Journey"], Chekist.ru, March 31, 2006, http://chekist.ru/article/1326.

106 MI5, Compilation of Ginzberg's MI5 debriefings. "Information Obtained from General Krivitsky," 9.

107 Alexander Barmine, *One Who Survived: The Life Story of a Russian Under the Soviets* (New York: G. P. Putnam's Sons, 1945), 7.

108 Walter Krivitsky, *I Was Stalin's Agent* (London: Hamish Hamilton, 1939), 245-47.

109 Ismail Akhmedov, *In and Out of Stalin's GRU: A Tatar's Escape from Red Army Intelligence* (Frederick, MD: University Publications of America, 1984), 137.

110 Salikhov, "From Registupr to GRU."

111 Oleg Nazhestkin, "Предисолвия" ["Foreword"], in Yevgeniy Primakov, ed., *Очерки истории российской внешней разведки* [*Essays on the History of Russian Foreign Intelligence*], vol. 3 (Moscow: Mezhdunarodniye Otnosheniya, 2003), 9.

112 Salikhov, "From Registupr to GRU."

113 Presidium of the Central Committee of the CPSU, "Положение о Комитете государственной безопасности при Совете Министров СССР и его органах на местах" ["Resolution on the Committee of State Security of the USSR Council of Ministers and Its Local Bodies"], January 9, 1959.

114 Petr Deryabin and Frank Gibney, *The Secret World* (New York: Doubleday, 1959), 63.

115 Vladimir Soldatkin and Christian Lowe, "Russia Orders Out 60 U.S. Diplomats Over Spy Poisoning Affair," Reuters, March 20, 2018, https://www.reuters.com/article/us-russia-diplomats/russia-orders-out-60-u-s-diplomats-over-spy-poisoning-affair-idUSKB N1H52MN.

116 Julie Fedor, "Chekists Look Back on the Cold War: The Polemical Literature," *Intelligence and National Security* 26, no. 6 (December 2011): 842-63.

117 Jens, "Cold War Spy Fiction in Russian Popular Culture," 31-41.

118 "В МИД России пожаловались на 'план Даллеса'" ["Complaints about the 'Dulles Plan' at the MFA"], Lenta.ru, May 14, 2020, https://lenta.ru/news/2020/05/14/dalles/.

119 "K.G.B. Passes Secrets Back to U.S.," *New York Times*, December 14, 1991, 1

120 Martin Ebon, *KGB: Death and Rebirth* (Westport, CT: Praeger, 1994), 61-62.

121 Andrey Kozyrev, "Stand By Us," Editorial, *Washington Post*, August 21, 1991, https://www.washingtonpost.com/archive/opinions/1991/08/21/stand-by-us/54b27a33-96b7-4bf2-b8a4-113ddb03f38b/.

122 James Sherr, "Yet Another Reorganization," *Janes Intelligence Review*, August 1, 1995.

123 Maria Lipman, "How Putin Silences Dissent," *Foreign Affairs* 95, no. 3 (May/June 2016): 38-46, https://www.foreignaffairs.com/articles/russia-fsu/2016-04-18/how-putin-silences-dissent.

124 Valeriy Velichko, *От Лубянки до Кремля: Секретные Миссии* [*From Lubyanka to the Kremlin: Secret Missions*] (Moscow: Akva-Term, 2013), http://nastural.ru/uploadedFiles/files/biblioteka/Ot_Lubyanki_do_Kremlya._V.Velichko.pdf.

125 Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services* (London: European Council on Foreign Relations, 2016), 5, https://ecfr.eu/archive/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf.

126 Vyacheslav Fronin, "ФСБ расставляет акценты" ["The FSB Sets the Accents"], *Rossiyskaya Gazeta*, December 19, 2017, https://rg.ru/2017/12/19/aleksandr-bortnikov-fsb-rossii-svobodna-ot-politicheskogo-vliianiia.html.

127 Lezina, "Dismantling the State Security Apparatus," 12.

128 Sherr, "Yet Another Reorganization," citing a press conference by then-FSK Director Sergey Stepashin.

129 Ilan Berman and J. Michael Waller, eds., *Dismantling Tyranny: Transitioning Beyond Totalitarian Regimes* (Lanham, MD: Rowman and Littlefield, 2006), 23.

130 Anna Nemtsova, "A Chill in the Moscow Air," *Newsweek*, February 5, 2006, https://www.newsweek.com/chill-moscow-air-113415.

131 Russia Foreign Intelligence Service (SVR) website, www.svr.gov.ru.

132 "Рогозин опубликовал фото с бойцами 'Заслона' в Сирии" ["Rogozin Published a Photo with 'Zaslon' Soldiers in Syria"], *Vzglyad*, May 24, 2014, https://vz.ru/news/2014/5/24/688286.html.

133 “Спецназ СВР” [“SVR Spetsnaz”], Agentura.ru, http://www.agentura.ru/dossier/russia/svr/specnaz/.

134 “Глава СВР Нарышкин подтвердил, что в советские времена работал в Брюсселе” [“SVR Chief Confirmed That During the Soviet Times He Worked in Brussels”], *RIA Novosti*, September 5, 2020, https://ria.ru/20200905/naryshkin-1576816627.html.

135 David Remnick, “KGB Targeted for Major Reform,” *Washington Post*, August 27, 1991.

136 Korenkov, ed., *Military Counterintelligence of the FSB*, 36.

137 Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015), 125-27; see also Yuriy Sinodov, “Грязные руки” [“Dirty Hands”], Roem.ru, July 18, 2011, https://roem.ru/18-07-2011/120190/gryaznye-ruki/.

138 U.S. Department of Justice, “U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts,” Press Release, March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

139 Scott Shane, David E. Sanger, and Andrew E. Kramer, “Russians Charged With Treason Worked in Office Linked to Election Hacking,” *New York Times*, January 27, 2017, https://www.nytimes.com/2017/01/27/world/europe/russia-hacking-us-election.html.

140 Charlie Osborne, “Russian APT Turla Targets 35 Countries on the Back of Iranian Infrastructure,” *Zero Day*, October 21, 2019, https://www.zdnet.com/article/russian-apt-turla-targets-35-countries-on-the-back-of-iranian-infrastructure/.

141 CrowdStrike, *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed* (Sunnyvale, CA: CrowdStrike, 2020), 36.

142 Andrew and Mitrokhin, *The Sword and the Shield*, 389.

143 “‘V’ for ‘Vympel’: FSB’s Secretive Department ‘V’ Behind Assassination of Georgian Asylum Seeker In Germany,” *Bellingcat*, February 17, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/.

144 Russian Federation, “Questions of Federal Service of the Protection of the Russian Federation,” Order of the President of the Russian Federation, August 7, 2004, N 1013, http://www.consultant.ru/document/cons_doc_LAW_48778/.

145 “ФСО” [“FSO”], Voenpro.ru, October 22, 2013, https://voenpro.ru/infolenta/fco.

146 “Новый глава ФСО Кочнев служит в органах госохраны 14 лет” [“New FSO Chief Kochnev Has Served in the State Protection Organs for 14 Years”], *TASS*, May 26, 2016, https://tass.ru/politika/3317285.

147 Sergey Sukhankin, “Russian National Guard: A New Oprichnina, ‘Cyber Police’ or Something Else?” *Eurasia Daily Monitor* 14, no. 38 (March 21, 2017): https://jamestown.org/program/russian-national-guard-new-oprichnina-cyber-police-something-else-2/.

148 Olga Vetrova, "Росгвардия усмотрела схожесть протестов в РФ с 'цветными' революциями" ["The Russian National Guard Sees a Similarity between Protests in the RF and 'Color' Revolutions"], *New Day*, June 16, 2017, https://newdaynews.ru/moskow/606096.html.

149 "Ex-FSB chief: Russian National Guard Creation Important Amid Nato's Eastward Expansion," *TASS*, May 17, 2016, https://tass.com/politics/876141.

150 Sergey Khazov-Kassia, "Человек за Спиной" ["The Man Behind the Back"], *New Times*, November 17, 2014, https://newtimes.ru/articles/detail/90102.

151 Aleksandr Kudryavtsev, "Генерал Армии Виктор Золотов: 'Росгвардия Работает Для Людей'" ["Army General Viktor Zolotov: 'Rosgvardiya Works for the People'"], *Voenniy*, no. 4 (2017), https://rosguard.gov.ru/ru/page/index/zhurnal-voennyj-4-general-armii-viktor-zolotov-rosgvardiya-rabotaet-dlya-lyudej; see also Peter Earley, *Comrade J: The Untold Secrets of Russia's Mystery Spy in America After the End of the Cold War* (New York: Berkley Books, 2007), 298-301.

152 "CrowdStrike's Work with the Democratic National Committee: Setting the Record Straight," *CrowdStrike*, June 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

153 Sergey Operov and Ivan Safronov, "Министерство чрезвычайных полномочий: Готовится реформа правоохранительных и силовых структур" ["Ministry of Emergency Powers: A Reform of Law Enforcement and Power Structures is Being Prepared"], *Kommersant*, June 19, 2016, https://www.kommersant.ru/doc/3093174.

154 Dmitriy Abzalov, "У ФСО достаточно широкие возможности" ["The FSO Has Broad Enough Opportunities"], *Kommersant*, September 25, 2016, https://www.kommersant.ru/doc/3154835.

155 Vyacheslav Polovinko and Lilit Sarkisyan, "The FSB Gathers Up the Keys to 'Yandex,'" *Novaya Gazeta*, June 5, 2019, 2.

156 Ivan Nechepurenko, "New Spies Went for a Joyride in Moscow. Russia Isn't Happy," *New York Times*, July 14, 2016, https://www.nytimes.com/2016/07/15/world/europe/russia-fsb-security-service.html; "Rookie FSB agents Are Punished for 'Indecent' Graduation Jinx in Moscow," *Siberian Times*, August 2, 2016, https://siberiantimes.com/home/sent-to-siberia/s0025-rookie-fsb-agents-are-punished-for-indecent-graduation-jinx-in-moscow/.

157 Filip Kovacevic, "How Russia Trains its Spies: The Past and Present of Russian Intelligence Education," in Liam Francis Gearon, ed., *The Routledge International Handbook of Universities, Security and Intelligence Studies* (London: Routledge, 2019), 187-95.

158 Christo Grozev, "FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning," *Bellingcat*, December 14, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/; Daria Litvinova, "Navalny Releases Recording of Call to

his Alleged Poisoner," *AP News*, December 21, 2020, https://apnews.com/article/alexei-navalny-poisoning-underpants-202f470c2d1c19151b9deb564d94e8f9.

159 Orlov, *Handbook of Intelligence and Guerrilla Warfare*.

160 "Заседание коллегии ФСБ России" ["Conference of the FSB Collegium of Russia"], Kremlin.ru, February 24, 2021, http://www.kremlin.ru/events/president/news/65068.

161 "Заседание коллегии ФСБ" ["Conference of the FSB Collegium"], Kremlin.ru, February 20, 2020, http://kremlin.ru/events/president/news/62834.

162 Nathan Hodge et al., "Russia Detains US citizen Paul Whelan on Suspicion of Spying," *CNN*, December 31, 2018, https://www.cnn.com/2018/12/31/us/russia-detains-us-citizen/index.html.

163 Katelyn Polantz, Veronica Stracqualursi, and Marshall Cohen, "Alleged Russian Spy Maria Butina Pleads Guilty To Engaging in Conspiracy Against US," *CNN*, December 13, 2018, https://www.cnn.com/2018/12/13/politics/maria-butina-guilty-plea/index.html.

164 Committee for State Security, "The KGB's 1967 Annual Report," May 6, 1968, Center for Preservation of Contemporary Documentation (TsKhSD), f. 89, op. 5, d. 3, ll. 1-14. Translated by Vladislav Zubok for the Wilson Center Cold War Intelligence History Project, History and Public Policy Program Digital Archive, http://digitalarchive.wilsoncenter.org/document/110403.

165 Cable to Foreign Office reporting initial interrogation of Aleksandr Zhigunov, dated August 27, 1942, in "Testimony of the NKVD Official Zhigunov," 8, 16, German file number EAP 3-a-11/2; National Archives and Records Administration, RG 242, Entry UD 282AV, Box 18.

166 "Testimony of the NKVD Official Zhigunov," 15-16; see also Zhigunov article, "English Intelligence in the USSR and the Activity of the English Embassy in Moscow," in "Testimony of the NKVD Official Zhigunov," 129-30.

167 Yuri Rastvorov, "Red Fraud and Intrigue in the Far East," *Life*, December 6, 1954, 182.

168 Australian Security Intelligence Organisation Memo, April 14, 1954, National Archives of Australia, A6283, folder 1, item number 4104669, 96.

169 Bagley, *Spymaster*, 4-8.

170 David Easter, "Soviet Bloc and Western Bugging of Opponents' Diplomatic Premises During the Early Cold War," *Intelligence and National Security* 31, no. 1 (2016): 28-48, https://www.tandfonline.com/doi/full/10.1080/02684527.2014.926745.

171 Central Intelligence Agency, "The Examination of the Bona Fides of a KGB Defector," February 1968, 310; available in National Archives and Records Administration, JFK Assassination Archives, document number 104-10150-10136.

172 Karavashkin, *Who Betrayed Russia*, 600.

173 Richards J. Heuer, Jr., "Nosenko: Five Paths to Judgment," in H. Bradford Westerfield, *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992* (New Haven: Yale University Press, 1995), 408.

174 "Spies Without Borders—How the FSB Infiltrated the International Visa System," *Bellingcat*, November 16, 2018, https://www.bellingcat.com/news/uk-and-europe/2018/11/16/spies-without-borders-fsb-infiltrated-international-visa-system/.

175 Nick Hopkins, "Suspected Russian Spy Found Working at US Embassy in Moscow," *Guardian*, August 2, 2018, https://www.theguardian.com/us-news/2018/aug/02/suspected-russian-spy-us-embassy-moscow-secret-service.

176 Sean Lyngaas, "Russian Intelligence-Backed Hackers Go After Armenian Embassy Website with New Code," *Cyberscoop*, March 12, 2020, https://www.cyberscoop.com/turla-fsb-eset-armenia/.

177 Alberto Nardelli, "The EU's Embassy in Russia Was Hacked but the EU Kept It a Secret," *BuzzFeed*, June 5, 2019, https://www.buzzfeednews.com/article/albertonardelli/eu-embassy-moscow-hack-russia.

178 Andrew Blake, "Russia-linked Hacking Group Targeting North Americans and European Diplomats: Report," *AP News*, February 28, 2018, https://apnews.com/article/574b09ffc262cb2edbfce7c4c0f9cd46.

179 U.S. Department of State, "Department of State Actions in Response to Russian Harassment," December 29, 2016, https://2009-2017.state.gov/r/pa/prs/ps/2016/12/266145.htm; Antonio and Jonna Mendez, *The Moscow Rules: The Secret CIA Tactics that Helped America Win the Cold War* (New York: Hatchette Book Company, 2019).

180 "Russia 'Ends Chechnya Operation,'" *BBC*, April 16, 2009, http://news.bbc.co.uk/2/hi/europe/8001495.stm.

181 "Заседание коллегии ФСБ России" ["Conference of the FSB Collegium of Russia"], Kremlin.ru, February 24, 2021, http://www.kremlin.ru/events/president/news/65068.

182 Ministry of Foreign Affairs of the Russian Federation, *Foreign Policy Concept of the Russian Federation*, December 1, 2016.

183 Ministry of Foreign Affairs of the Russian Federation, "Foreign Policy Concept."

184 "US Provided Information on Terrorist Plotters in Russia, Says FSB Chief," *TASS*, October 17, 2019, https://tass.com/politics/1083742.

185 Steffany A. Trofino, "Dagestan: Moscow's Risk Versus Gain," *International Journal of Intelligence and CounterIntelligence* 24, no. 2 (2011): 253–67.

186 Tony Halpin, "Gunmen Kill Seven Women in Russian Sauna," *Times* (London), August 14, 2009.

187 Yevgeniy Krutikov "Российская нелегальная разведка остается предметом зависти Запада" ["Russian Illegal Intelligence Remains an Object of Envy in the West"], *Vzglyad*, July 29, 2017, https://vz.ru/politics/2017/6/29/876627.html.

188 Oliver Stone, *The Putin Interviews* (New York: Hot Books, 2017), 36.

189 Deryabin and Gibney, *The Secret World*, 63.

190 Egbert Jahn, "The Castling of Presidential Functions by Vladimir Putin," in *International Politics: Political Issues Under Debate*, vol. 1 (Berlin: Springer, 2015), 107-22.

191 Egor Vinogradov, “Движение ‘За честные выборы’ начало новую серию протестов” [“The ‘For Honest Elections’ Movement Began a New Series of Protests”], *Deutsche Welle* (in Russian), March 6, 2012.

192 Ellen Barry and Michael Schwirtz, “Arrests and Violence at Overflowing Rally in Moscow,” *New York Times*, May 6, 2012, https://www.nytimes.com/2012/05/07/world/europe/at-moscow-rally-arrests-and-violence.html.

193 Mischa Gabowitsch, *Protest in Putin's Russia* (Malden, MA: Polity Press, 2017), 11.

194 “Yarovaya Law Obliges Operators and Internet Companies To Store User Correspondence,” *TASS*, July 1, 2018, https://tass.com/politics/1011585.

195 “Russia: ‘Big Brother’ Law Harms Security, Rights,” *Human Rights Watch*, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

196 “‘Яндекс’ подтвердил наличие решения по ключам шифрования для ФСБ” [“Yandex Confirmed Having Reached a Solution to Encryption Keys for the FSB”], *RBC*, June 7, 2019, https://www.rbc.ru/society/07/06/2019/5cfa2a169a7947affada5b1a.

197 “Who's Asking? ‘Yandex’ Releases First-ever Transparency Report on Requests for User Data From the Russian Authorities,” *Meduza*, October 26, 2020, https://meduza.io/en/feature/2020/10/26/who-s-asking.

198 Jane Wakefield, “Russia ‘Successfully Tests’ Its Unplugged Internet,” *BBC*, December 24, 2019, https://www.bbc.com/news/technology-50902496.

199 Orlov, *Handbook of Intelligence and Guerrilla Warfare*, 14.

200 Christopher Andrew and Oleg Gordievsky, *Comrade Kryuchkov's Instructions: Top Secret Files on KGB Foreign Operations, 1975-1985* (Stanford, CA: Stanford University Press, 1993), 9.

201 Jason Lewis, “Russian Spy Targeted MPs and Whitehall Officials,” *Telegraph*, December 10, 2011, https://www.telegraph.co.uk/news/worldnews/europe/russia/8948359/Russian-spy-targeted-MPs-and-Whitehall-officials.html.

202 U.S. Director of National Intelligence, *Vision 2015: A Globally Networked and integrated intelligence Enterprise* (Washington, DC: Office of the Director of National Intelligence, 2015), https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Vision_2015.pdf.

203 Andrew and Gordievsky, *Comrade Kryuchkov's Instructions*, 17.

204 Andrew and Gordievsky, *Comrade Kryuchkov's Instructions*, 17.

205 Ministry of Foreign Affairs of the Russian Federation, *Foreign Policy Concept,* 3.

206 Vladimir Putin, “Being Strong: Why Russia Needs To Rebuild Its Military,” *Foreign Policy*, February 21, 2012, https://foreignpolicy.com/2012/02/21/being-strong/.

207 Quoted in Condoleezza Rice, “The Making of Soviet Strategy,” in Peter Paret, ed., *Makers of Modern Strategy from Machiavelli to the Nuclear Age* (Princeton: Princeton University Press, 1986), 661.

208 Council on Foreign Relations, Cyber Operations Tracker, https://www.cfr.org/interactive/cyber-operations.

209 Earley, *Comrade J*, 224-39.

210 Earley, *Comrade J*, 228.

211 Corera, *Russians Among Us*, 220-21.

212 Ben Smith, "Clinton Friend Was Spy's Target," *Politico*, June 29, 2010, https://www.politico.com/blogs/ben-smith/2010/06/clinton-friend-was-spys-target-027850.

213 Corera, *Russians Among Us*, 270.

214 Pablo Gorondi, "Hungarian Politician on Trial for Spying on EU for Russia," *AP News*, July 10, 2018, https://apnews.com/article/3fa4f9b515034ab196dbb49fa6e9056e.

215 "Bulgaria Charges Former Lawmaker With Spying for Russia," *Radio Free Europe/Radio Liberty*, September 10, 2019, https://www.rferl.org/a/bulgaria-charges-former-lawmaker-with-spying-for-russia/30157289.html; "Bulgarian NGO Official Charged With Spying for Russia," *Reuters*, September 10, 2019, https://www.reuters.com/article/us-bulgaria-russia-espionage/bulgarian-ngo-official-charged-with-spying-for-russia-idUSKCN1VV1W7.

216 U.S. Congress, Senate, Committee on Foreign Relations, *Russian Intelligence Activities Directed at the Department of State*, 106th Congress, Second Session, February 10, 2000 (Washington, DC: Government Printing Office, 2000).

217 "How Russian Spies Bugged the US State Department," *CNN*, October 23, 2019, https://www.cnn.com/2017/08/23/us/spyhunter-russia-bug-us-state-department-declassified/index.html.

218 "Swiss Police 'Exposed Russian Spies in Davos,'" *BBC*, January 21, 2020, https://www.bbc.com/news/world-europe-51196659; Chris Baynes, "Russian Spies Found 'Posing as PLUMBERS' in Davos, Report Says," *Independent*, January 21, 2020, https://www.independent.co.uk/news/world/europe/davos-2020-russia-spies-plumbers-switzerland-wef-a9295076.html.

219 Mirek Tóda, "A Russian Spy's Manual: Send a Secret Message to the Strela-3 Satellite and Betray NATO Allies," *Dennik N*, October 11, 2020, https://dennikn.sk/2082755/russian-spys-manual-send-a-secret-message-to-the-strela-3-satellite-and-betray-nato-allies/.

220 "Former Official Arrested for Treason," *Baltic Times*, September 22, 2008, https://www.baltictimes.com/news/articles/21387/.

221 U.S. District Court, Eastern District of Virginia, "USA v. Peter Rafael Dzibinski Debbins, aka 'Ikar Lesnikov,'" August 20, 2020, https://www.justice.gov/opa/press-release/file/1307186/download.

222 Nova Scotia Department of Justice, Pre-Sentence Report, "Queen v. Jeffrey Paul Delisle," December 28, 2012, https://assets.documentcloud.org/documents/602196/delisles-pre-sentence-report.pdf; "Russian mole had access to wealth of CSIS, RCMP, Privy Council files," *The Globe and Mail*, October 22, 2012, https://www.theglobeandmail.com/news/politics/russian-mole-had-access-to-wealth-of-csis-rcmp-prive-council-files/article4627659/.

223 "Russian Spy Raymond Poeteray Jailed by Dutch," *BBC*, April 23, 2013, https://www.bbc.com/news/world-europe-22265494; "Dutch Diplomat Gets 12 Years for Spying for

Russia," *Moscow Times*, April 22, 2013, https://www.themoscowtimes.com/2013/04/22/dutch-diplomat-gets-12-years-for-spying-for-russia-a23551.

224 "Media: podejrzany o szpiegostwo na rzecz Rosji pracował w Agencji Mienia Wojskowego" ["Media: The Person Arrested for Espionage for Russia Worked in the Agency of Military Property"], *Polskie Radio*, October 28, 2019, https://polskieradio24.pl/5/1222/Artykul/2392622,ABW-zatrzymala-Piotra-S-Jest-podejrzany-o-szpiegostwo-na-rzecz-Rosji; Edyta Żemła, "Piotr Ś. mógł przekazać Rosji plany NATO-wskiej dywizji w Polsce" ("Piotr Ś. Could Provide Russia the Plans for a NATO Division in Poland"), *Onet News*, November 2, 2019, https://wiadomosci.onet.pl/kraj/piotr-s-mogl-przekazac-rosji-plany-nato-wskiej-dywizji-w-polsce/q0dxdyn.

225 Corera, *Russians Among Us*, 127, 216-17.

226 Robert S. Mueller, *The Mueller Report: Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Brooklyn, NY: Melville House, 2019).

227 Kellock-Taschereau Commission, *Report of the Royal Commission Appointed under Order in Council P.C. 411 of February 5, 1946 to Investigate the Facts Relating to and the Circumstances Surrounding the Communication by Public Officials and Other Persons in Positions of Trust of Secret and Confidential Information to Agents of a Foreign Power* (Ottawa: Privy Council, 1946), 115-16.

228 Main Intelligence Directorate (GRU) of the Soviet Armed Forces General Staff, Ottawa to Moscow, GRU Telegram number 209, dated July 12, 1945; The National Archives, Kew, London, KV 2/1247, item 73.

229 "Register of Materials Sent to the Director," dated January 1945, The National Archives, Kew, London, KV 2/1427, serial 8a, item 108.

230 Kalugin, *Spymaster*, 100-02.

231 Christopher Andrew and Vasili Mitrokhin, *The World Was Going Our Way: The KGB and the Battle for the Third World* (New York: Basic Books, 2005), 19.

232 "Germany Fighting Off Spy Onslaught," *New York Herald Tribune*, October 8, 1961.

233 Jason Lewis, "The Traitor in a Headscarf: How Czech Spy Agent Hammer Worked Secretly Inside Parliament for Years," *Daily Mail*, November 15, 2008, https://www.dailymail.co.uk/news/article-1086187/The-traitor-headscarf-How-Czech-spy-Agent-Hammer-worked-secretly-inside-Parliament-years.html.

234 Glen Owen, "Labour MP Pulled Before Chief Whip for Inviting 'Russian Spy' to Tea in the Commons," *Daily Mail*, June 28, 2008, https://www.dailymail.co.uk/news/article-1030235/Labour-MP-pulled-chief-whip-inviting-Russian-spy-tea-Commons.html.

235 Jason Lewis, "Mikhail Repin: The Perfect Party Guest Who Was Whitehall Spy for the Russians," *Telegraph,* December 10, 2011, https://www.telegraph.co.uk/news/worldnews/europe/russia/8948357/Mikhail-Repin-the-perfect-party-guest-who-was-Whitehall-spy-for-the-Russians.html; Lewis, "Russian Spy Targeted MPs and Whitehall Officials."

236 "Russian 'Spy' Katia Zatuliveter: MP Lover Paid for Trips," *BBC*, October 27, 2011, https://www.bbc.com/news/uk-15476077; Lewis, "Russian Spy Targeted MPs and Whitehall Officials."

237 "U.S. Hits Russian Oligarchs and Officials with Sanctions Over Election Interference," *NPR*, April 6, 2018, https://www.npr.org/sections/thetwo-way/2018/04/06/600083466/u-s-hits-russian-oligarchs-and-officials-with-sanctions-over-election-interferen.

238 Mike McIntire, "Billionaire Backer of Maria Butina Had Russian Security Ties," *New York Times*, September 21, 2018, https://www.nytimes.com/2018/09/21/us/politics/maria-butina-russian-oligarch.html.

239 Josh Meyer, "Accused Russian Agent Met with Suspected Kremlin Spy," *Politico*, July 28, 2018, https://www.politico.com/story/2018/07/28/mariia-butina-russia-kremlin-suspected-spy-746043.

240 "Public Diplomacy's 90th Anniversary at RCSC," *Russian Beyond*, November 20, 2015, https://www.rbth.com/arts/culture/2015/11/20/public-diplomacys-90th-anniversary-at-rcsc_542417.

241 See for example, Central Intelligence Agency, "Soviet-Sponsored Societies of Friendship and Cultural Relations," October 1957, CIA FOIA Reading Room; Aleksandr Y. Kaznacheyev, "Soviet 'Operation Burma,'" *The New Leader*, January 18, 1960, 41-42.

242 "Maria Butina: The Russian Gun Activist Who Was Jailed in the US," *BBC*, October 25, 2019, https://www.bbc.com/news/world-us-canada-44885633.

243 Gordon Corera, "Russia Report: What Would Tougher Spy Laws Mean for UK?," *BBC*, July 22, 2020, https://www.bbc.com/news/uk-53502905.

244 "From Espionage to Cyber Propaganda: Pawn Storm's Activities over the Past Two Years," *TrendMicro*, April 25, 2017, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm; "German Media: Cyber Attack Carried Out on Bundestag," *Deutsche Welle*, May 15, 2015, https://www.dw.com/en/german-media-cyber-attack-carried-out-on-bundestag/a-18452770; "Germany Admits Hackers Infiltrated Federal Ministries, Russian Group Suspected," *Deutsche Welle*, February 28, 2018, https://www.dw.com/en/germany-admits-hackers-infiltrated-federal-ministries-russian-group-suspected/a-42775517; "The Labor Party Exposed to Hostile Hacker Attacks," TV2.no, February 2, 2017, https://www.tv2.no/nyheter/8902520/.

245 "German Man Charged with Giving Bundestag Floor Plans to Russian Intelligence," *Reuters*, February 25, 2021, https://www.reuters.com/article/us-germany-security-russia/german-man-charged-with-giving-bundestag-floor-plans-to-russian-intelligence-idUSKBN2AP11E.

246 Jan M. Olsen, "Norway Says Russia Was Behind Hacker Attack on Parliament," *AP News*, October 14, 2020, https://apnews.com/article/technology-oslo-russia-denmark-hacking-4c177f74287ab69816b954f8793e26c1.

247 "Матвиенко назвала задержание Бочкарева в Норвегии провокацией" ["Matvienko Called Bochkarev's Arrest in Norway a Provocation"], *RIA Novosti*, October 22, 2018.

248 Atle Staalesen, "Mikhail Bochkarev Is Released, Norwegian Security Police Might Drop Espionage Charges," *Barents Observer*, October 19, 2018, https://thebarentsobserver.com/en/life-and-public/2018/10/mikhail-bochkarev-released-norwegian-security-police-drops-espionage-charges.

249 Ivo Juurvee and Lavly Perling, *Russia's Espionage in Estonia: A Quantitative Analysis of Convictions* (Tallinn, Estonia: International Centre for Defense and Security, 2019).

250 Ian Cobain, "Boris Berezovsky Inquest Returns Open Verdict on Death," *Guardian*, March 27, 2014, https://www.theguardian.com/world/2014/mar/27/boris-berezovsky-inquest-open-verdict-death.

251 Feike Hacquebord, "Pawn Storm Targets MH17 Investigation Team," *Trendmicro*, October 22, 2015, https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/.

252 "Belling the BEAR," *Threat Connect*, September 28, 2016, https://threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/.

253 Chris Bing, "APT28 Targeted Montenegro's Government Before It Joined NATO, Researchers Say," *Cyberscoop*, June 6, 2017, https://www.cyberscoop.com/apt28-targeted-montenegros-government-joined-nato-researchers-say/.

254 Costas Kantouris and Menelaos Hadjicostis, "Greece: Russians Expelled Over Cash-for-Protests Allegation," *AP News*, July 12, 2018, https://apnews.com/article/aaf032985e7341d3a7968f6ff6b95ce0.

255 U.S. District Court, Western District of Pennsylvania, "USA v. Aleksei Sergeyevich Morenets et al.," Case 2:18-cr-00263-MRH, March 10, 2018, https://www.justice.gov/opa/page/file/1098481/download; "Dutch Government Says It Disrupted Russian Attempt To Hack Chemical Weapons Watchdog," *CNBC*, October 4, 2018, https://www.cnbc.com/2018/10/04/dutch-government-disrupted-russian-attempt-to-hack-chemical-weapons-watchdog.html.

256 Zack Whittaker, "Bellingcat Journalists Targeted by Failed Phishing Attempt," *Tech Crunch*, July 27, 2019, https://techcrunch.com/2019/07/27/bellingcat-targeted-failed-phishing-attempt/.

257 World Anti-Doping Agency, "WADA Confirms Attack by Russian Cyber Espionage Group," Press Release, September 13, 2016, https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group.

258 U.S. District Court, Western District of Pennsylvania, "USA v. Aleksei Sergeyevich Morenets, et al;" Catalin Cimpanu, "German Authorities Charge Russian Hacker for 2015 Bundestag Hack," *Zero Day*, May 5, 2020, https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/.

259 Raymond L. Garthoff, *Soviet Leaders and Intelligence: Assessing the American Adversary during the Cold War* (Washington, DC: Georgetown University Press, 2015), 74-94.

260 Ministry of Foreign Affairs of the Russian Federation, *Foreign Policy Concept*, 1.

261 Putin, "Being Strong."

262 National Counterintelligence Center, *Annual Report to Congress on Economic Collection and Industrial Espionage* (Washington, DC: NACIC, 1995).

263 Defense Security and Counterintelligence Agency, *Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry* (Washington, DC: DSCA, 2019).

264 Gary Kern, *A Death in Washington* (New York: Enigma Books, 2003), 34.

265 Brian R. Sullivan, "Soviet Penetration of the Italian Intelligence Services in the 1930s," in Tomaso Vialardi di Sandigliano and Virgilio Ilari, eds., *The History of Espionage: Italian Military Intelligence, Electronic Intelligence, Chinese Intelligence* (Biella, Italy: Associazione Europea degli Amici degli Archivi Storici, 2005), 87.

266 MI5, Compilation of Ginzberg's MI5 debriefings. "Information Obtained from General Krivitsky," 16.

267 Cross-reference from MI6 Intelligence Reports dated May 23 and May 24, 1933, The National Archives, Kew, London, KV 2/1898, serial 2a; "Ignace Reiss Personal History," dated October 17, 1949, The National Archives, KV 2/1898, serial 15a.

268 Barmine, *One Who Survived*, 173.

269 Federal Bureau of Investigation, "Iosif Volodarsky," Investigative Summary, The National Archives, Kew, London, KV 2/2881, serial 115a, 53.

270 Federal Bureau of Investigation, "Iosif Volodarsky," Investigative Summary, 23.

271 Haynes, Klehr, and Vassiliev, *Spies: The Rise and Fall of the KGB in America*, 384, citing Volodarsky's FBI interrogation.

272 Orlov, *Handbook of Intelligence and Guerrilla Warfare*, 32. The NKVD (People's Commissariat of Internal Affairs) housed the Soviet Union's civilian foreign intelligence apparatus at the time.

273 Andrew and Mitrokhin, *The Sword and the Shield,* 218.

274 Viktor Suvorov, *Aquarium: The Career and Defection of a Soviet Military Spy* (London: Hamish Hamilton, 1985), 139-58.

275 Gus W. Weiss, "The Farewell Dossier: Duping the Soviets," *Studies in Intelligence* 39, no. 5 (1996).

276 Amy Knight, *Spies without Cloaks: The KGB's Successors* (Princeton: Princeton University Press, 2001), 121-22.

277 Sue Somers, "Ik vind nietdat ik iets anti-Belgisch heb gedaan" ["I Don't Think I've Done Anything Anti-Belgian"], *DeMorgen*, July 16, 2011, https://www.demorgen.be/nieuws/ik-vind-nietdat-ik-iets-anti-belgisch-heb-gedaan~b95a6b30/; Adam Zagorin, "Still Spying After All These Years," *Time*, June 29, 1992.

278 Andrew and Mitrokhin, *The Sword and the Shield*, 218.

279 Zach Dorfman, "The Secret History of the Russian Consulate in San Francisco," *Foreign Policy*, December 14, 2017, https://foreignpolicy.com/2017/12/14/the-secret-history-of-the-russian-consulate-in-san-francisco-putin-trump-spies-moscow/; see also Canadian Broadcasting Corporation, "The KGB Connections: An Investigation in Soviet Operations in North America," Documentary, 1982, https://www.youtube.com/watch?v=diT9oQjb8Ik, which also claimed the San Francisco consulate was capable of intercepting microwave communications in Silicon Valley and in New York.

280 National Intelligence Council, *The Technology Acquisition Efforts of the Soviet Intelligence Services*, Interagency Intelligence Memorandum, June 1982, 3, referencing CIA Crest Program.

281 Zach Dorfman, "How Silicon Valley Became a Den of Spies," *Politico*, July 27, 2018, https://www.politico.com/magazine/story/2018/07/27/silicon-valley-spies-china-russia-219071.

282 Carl Schreck, "FBI Wary Of Possible Russian Spies Lurking In U.S. Tech Sector," *Radio Free Europe/Radio Liberty*, May 17, 2014, https://www.rferl.org/a/fbi-wary-of-possible-russian-spies-in-lurking-in-us-tech-sector/25388490.html.

283 U.S. Department of Justice, "Brooklyn Resident and Two Russian Nationals Arrested in Connection with Scheme to Illegally Export Controlled Technology to Russia," Press Release, October 6, 2016, https://www.justice.gov/opa/pr/brooklyn-resident-and-two-russian-nationals-arrested-connection-scheme-illegally-export; U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases (January 2016 to the present: updated January 2019)," January 2019, 34-35, https://www.hsdl.org/?view&did=825543.

284 U.S. Department of Justice, "Exporter Of Microelectronics To Russian Military Sentenced To 135 Months In Prison Following Convictions On All Counts At Trial," Press Release, February 28, 2017, https://www.justice.gov/usao-edny/pr/exporter-microelectronics-russian-military-sentenced; U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases," 35-36.

285 ABN Universal Company website, accessed on March 11, 2021, http://www.abnuniversal.ru/content/page/company.htm.

286 U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases," 6-7.

287 Jan M. Olsen and Desmond Butler, "Russian Diplomat Accused of Espionage Quietly Leaves Sweden," *US News and World Report*, March 28, 2019.

288 U.S. District Court, Southern District of Ohio, *USA v. Alexander Yuryevich Korshunov*, August 21, 2019, https://www.globalsecurity.org/intell/library/news/2019/intell-190905-doj01_korshunov_complaint.pdf.

289 "Объединенная двигателестроительная корпорация подтвердила задержание своего сотрудника" ("United Engine Corporation Confirms the Arrest of its Employee"), *Interfax*, September 5, 2019.

290 "Russian 'Spy' Moved from Prison to House Arrest," *The Italian Insider*, December 3, 2019.

291 Fredrik Westerlund, *Russian Intelligence Gathering for Domestic R&D—Short Cut or Dead End for Modernisation?* (Stockholm: Swedish Defence Research Agency, 2010).

292 Sergey A. Vorontsov, *Спецслужбы России* [*Special Services of Russia*] (Rostov-na-Donu: Feniks, 2018), 412.

293 Orlov, *Handbook of Intelligence and Guerrilla Warfare*, 20.

294 Orlov, "The Theory and Practice of Soviet Intelligence," 53-54.

295 Cross-reference from MI6 Intelligence Reports dated May 23 and May 24, 1933; "Ignace Reiss Personal History," dated October 17, 1949, The National Archives, KV 2/1898, serial 15a.

296 Contact Report written by Marcus Weinstein, dated October 4, 1932, Volodarsky File, The National Archives, Kew, London, KV 2/2880, serial 19a; Contact Report written by Marcus Weinstein, dated October 12, 1932, Volodarsky File, The National Archives, KV 2/2880, serial 21a.

297 Aleksandr Brazhnev, *Школа Опричников* [*Oprichniki School*] (Kiev: Diokor, 2004), 65-66.

298 "George Kennan Telegram to Secretary of State," February 22, 1946, Document 475, in Rogers P. Churchill and William Slany, eds., *Foreign Relations of the United States, The Soviet Union*, Vol. VI (Washington, DC: Government Printing Office, 1969); "Russians Warned To Keep Vigilant; 'Capitalist Encirclement' Still Continues, Says Pravda in Urging Stronger Defenses," *New York Times*, March 19, 1953.

299 Aleksandr Khrolenko, "Военный бюджет США: что достанется Латвии" ["The US Defense Budget: What does Latvia Get"], Sputniknews.ru, February 12, 2020; see also Alexander Vershbow, NATO Deputy Secretary General, Speech in Trakai, Lithuania, January 15, 2016, https://www.nato.int/cps/en/natohq/opinions_127099.htm.

300 Karpov, *The Organization of the GPU*, 16-18.

301 Krivitsky, *I Was Stalin's Agent*, 135-58.

302 "Flood of Fake Bills Is Traced to Russia," *New York Times*, February 24, 1933; see also MI5 File on Valentine Gregory Burtan, The National Archives, Kew, London, KV 2/2673; Federal Bureau of Investigation (FBI), "Valentine Gregory Burtan, Internal Security–R," Investigative Summary, FBI file 100-262352, portions of which are cited in files stored in the FBI Vault.

303 Feldbin/Orlov discusses the counterfeit operation in U.S. Congress. Senate. Committee on the Judiciary. *Scope of Soviet Activity in the United States*, 85th Congress, First Session, Part 50, (Washington, DC: Government Printing Office, 1957), 3441-42.

304 U.S. Magistrate Judge, Southern District of New York, "USA v. Evgeny Buryakov, aka 'Zenya,' Igor Sporyshev, and Viktor Podobny," January 23, 2015, 5, https://storage.courtlistener.com/recap/gov.uscourts.nysd.438190/gov.uscourts.nysd.438190.1.0.pdf.

305 U.S. Magistrate Judge, Southern District of New York, "USA v. Evgeny Buryakov et al.," 14.

306 U.S. Department of Justice, "Evgeny Buryakov Pleads Guilty In Manhattan Federal Court In Connection With Conspiracy To Work For Russian Intelligence," Press Release,

March 11, 2016, https://www.justice.gov/usao-sdny/pr/evgeny-buryakov-pleads-guilty-manhattan-federal-court-connection-conspiracy-work.

307 U.S. Magistrate Judge, Southern District of New York, "USA v. Evgeny Buryakov et al.," 17.

308 U.S. Magistrate Judge, Southern District of New York, "USA v. Evgeny Buryakov et al.," 24.

309 "Russia's Rostec in Joint Venture Talks with Bombardier," *Reuters*, February 15, 2013, https://www.reuters.com/article/us-russia-rostec-bombardier/russias-rostec-in-joint-venture-talks-with-bombardier-idUSBRE91E0BW20130215.

310 Matthew Bodner, "Russian Spies May Have Pressured Canadian Union to Get Aircraft Deal," *Moscow Times*, January 27, 2015, https://www.themoscowtimes.com/2015/01/27/russian-spies-may-have-pressured-canadian-union-to-get-aircraft-deal-a43303.

311 U.S. Magistrate Judge, Southern District of New York, "USA v. Evgeny Buryakov et al.," 18-20.

312 "Bombardier Sees Delays in Joint-Venture with Russia's Rostec," *Reuters*, March 21, 2014, https://www.reuters.com/article/us-bombardier-rostec-idUSBREA2K1ZQ20140321; Jon Ostrower and Paul Vieira, "Bombardier Shelves Plans for Russian Assembly Line," *Wall Street Journal*, October 30, 2014, https://www.wsj.com/articles/bombardier-shelves-plans-for-russian-assembly-line-1414699181.

313 "Ex-SoftBank Employee Arrested Over Alleged Leak of Proprietary Information to Russian spies," *Japan Times*, January 26, 2020, https://www.japantimes.co.jp/news/2020/01/26/national/softbank-employee-arrested-leak-proprietary-information-russia-spies/#.XoyqWtNKgWo.

314 U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases," 98.

315 U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases," 48.

316 U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases," 7-8.

317 Earley, *Comrade J*, 210-17.

318 "EU Targets Syrian Middleman It Says Bought Oil From Islamic State," *Reuters*, March 8, 2015, https://www.reuters.com/article/syria-crisis-eu-idUSL5N0WA05R20150308#1uixRjmfedAEC25e.97.

319 U.S. Department of the Treasury, "Treasury Sanctions Networks Providing Support to the Government of Syria, Including for Facilitating Syrian Government Oil Purchases from ISIL," Press Release, November 25, 2015, https://www.treasury.gov/press-center/press-releases/Pages/jl0287.aspx.

320 Anna Nemtsova and Thomas Seibert, "Russia's ISIS Money Men Exposed," *The Daily Beast*, June26,2017,https://www.thedailybeast.com/russias-isis-money-men-exposed?ref=scroll.

321 Nina Khrushcheva, "Последний силовик?" ["The Latest Silovik?"], Inosmi.ru, December 4, 2017, https://inosmi.ru/politic/20171204/240916440.html.

322 Office of the U.S. Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, Intelligence Community Assessment, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

323 U.S. Magistrate Judge, Southern District of New York, "U.S.A. vs. Evgeny Buryakov et al."

324 "Lithuanian court upholds sentence for man convicted of spying for Russia," LRT.lt, January 17, 2020, https://www.lrt.lt/en/news-in-english/19/1134237/lithuanian-court-upholds-sentence-for-man-convicted-of-spying-for-russia.

325 Dirk Banse et al., "Circles of Power: Putin's Secret Friendship with ex-Stasi Officer," *Guardian*, August 13, 2014, https://www.theguardian.com/world/2014/aug/13/russia-putin-german-right-hand-man-matthias-warnig.

326 Andrea Shalal, "Russia-Germany Gas Pipeline Raises Intelligence Concerns—U.S. Official," *Reuters*, May 17, 2018, https://uk.reuters.com/article/uk-usa-germany-russia-pipeline/russia-germany-gas-pipeline-raises-intelligence-concerns-u-s-official-idUKKCN1II0V7.

327 L. Nikolayev, "Суд и Жизнь: 'Судебные Деятели'" ["The Court and Life: 'Judicial Officials'"], *Soviet Justice Weekly*, April 19, 1923, 349.

328 L. Nikolayev, "Суд и Жизнь: 'Следователь' Гершуни" ["The Court and Life: 'Inspector' Gershuni"], *Soviet Justice Weekly*, May 19, 1923, 444-45.

329 Karpov, The *Organization of the GPU.*

330 See, for example, Joint State Political Directorate (OGPU), "Спецсправка Секретно-политического отдела ОГПУ СССР "О ходе хлебозаготовок в Дальне-Восточном крае" по состоянию на 1 января 1933 г." ["Special Report of the Secret Political Section of the USSR OGPU 'On the Process of Bread Making in the Far Eastern Territory' on Conditions as of 1 January 1993"], January 13, 1933, Alexander Yakovlev Archive, https://www.alexanderyakovlev.org/fond/issues-doc/1025509; People's Commissariat for Internal Affairs (NKVD), "Спецсообщение Н.И. Ежова И.В. Сталину с приложением протокола допроса М.Л. Рухимовича ["Special Report of N. I. Yezhov to J. V. Stalin enclosing the interrogation protocol of M. L. Rukhimovich"], Alexander Yakovlev Archive, https://www.alexanderyakovlev.org/fond/issues-doc/61283.

331 Deryabin and Gibney, *The Secret World*, 63.

332 U.S. Coast Guard Atlantic Area, "Semper Vigilans: History of the USCGC Vigilant (WMEC-617)," https://www.atlanticarea.uscg.mil/Area-Cutters/CGCVIGILANT/History/.

333 Vladislav Krasnov, *Soviet Defectors: The KGB Wanted List* (Stanford, CA: Hoover Institution Press, 1985), 88.

334 U.S. Congress, House of Representatives, Committee on Foreign Affairs, Subcommittee on State Department Organization and Foreign Operations, *Attempted Defection by Lithuanian Seaman Simas Kudirka,* 91st Congress, Second Session (Washington, DC: Government Printing Office, 1970), 45.

335 Federal Bureau of Investigation (FBI), "Comments by Alexander Orlov Regarding Information Furnished by Walter Krivitsky," FBI Memo, The National Archives, Kew, London, KV 2/2879, serial 64b, 13.

336 Federal Bureau of Investigation, "Iosif Volodarsky," Investigative Summary.

337 Nick Paton Walsh, "Russia Says 'Spies' Work in Foreign NGOs," *Guardian*, May 13, 2005, https://www.theguardian.com/world/2005/may/13/russia.nickpatonwalsh.

338 Simon Saradzhyan and Carl Schreck, "NGOs a Cover for Spying in Russia," Globasresearch.ca, May 13, 2005, https://www.globalresearch.ca/ngos-a-cover-for-spying-in-russia/139.

339 Andrey Ostroukh, "Russia's Putin Signs NGO 'Foreign Agents' Law," *Reuters*, July 21, 2012, https://www.reuters.com/article/us-russia-putin-ngos/russias-putin-signs-ngo-foreign-agents-law-idUSBRE86K05M20120721.

340 "Profile: Mikhail Khodorkovsky," *BBC*, December 22, 2013, https://www.bbc.com/news/world-europe-12082222.

341 "Лубянская Федерация: Как ФСБ определяет политику и экономику России" ["The Lubyanka Federation: How the FSB Determines the Politics and Economics of Russia"], Dossier Center, 2020, https://fsb.dossier.center/.

342 Joshua Yaffa, "How Bill Browder Became Russia's Most Wanted Man," *The Atlantic*, August 13, 2018, https://www.newyorker.com/magazine/2018/08/20/how-bill-browder-became-russias-most-wanted-man.

343 Howard Amos, "Sergei Magnitsky's Posthumous Trial Gets Under Way in Russia," *Guardian*, March 22, 2013, https://www.theguardian.com/world/2013/mar/22/sergei-magnitsky-posthumous-trial-russia.

344 "Russian ex-minister Ulyukayev Gets Eight Years for Bribery," *BBC*, December 15, 2017, https://www.bbc.com/news/world-europe-42365041; Polina Nikolskaya and Darya Korsunskaya, "Russian Ex-minister Ulyukayev Jailed for Eight Years over $2 Million Bribe," *Reuters*, December 15, 2017, https://www.reuters.com/article/us-russia-ulyukayev-verdict/russian-ex-minister-ulyukayev-jailed-for-eight-years-over-2-million-bribe-idUSKBN1E90SN.

345 "Alexei Navalny: Russian Opposition Leader Found Guilty," *BBC*, February 8, 2013, https://www.bbc.com/news/world-europe-38905120.

346 "Russia Considers Stronger Secrecy Laws," *Financial Times*, October 30, 2015, https://www.ft.com/content/fc155bca-7f25-11e5-98fb-5a6d4728f74e.

347 Anna Baraulina, Evgenia Pismennaya, and Irina Reznik, "The Great Moscow Bank Shakedown," *Bloomburg*, December 10, 2019, https://www.bloomberg.com/news/articles/2019-12-10/russia-s-fsb-has-distorted-markets-and-sapped-investment.

348 "Were Top FSB Officials Jailed over Oligarchs' Struggle?" *Warsaw Institute*, April 27, 2019, https://warsawinstitute.org/top-fsb-officials-jailed-oligarchs-struggle/.

349 "The Rise and Fall of an FSB-Run Money Laundering Empire," *The Moscow Times*, August 3, 2019, https://www.themoscowtimes.com/2019/08/03/the-rise-and-fall-of-an-fsb-run-money-laundering-empire-a67226.

350 Janosh Neumann, interview by Andrew Hammond, Historian of the International Spy Museum, November 12, 2020.

351 Baraulina, Pismennaya, and Reznik, "The Great Moscow Bank Shakedown."

352 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (Washington, DC: ONCIX, 2011).

353 National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (Washington, DC: NCSC, 2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

354 U.S. Department of Justice, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," Press Release, October 4, 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

355 FireEye, *APT28: A Window into Russia's Cyber Espionage Operations?* (Milpitas, CA: FireEye, 2014), 3.

356 Huib Modderkolk, "Dutch Agencies Provide Crucial Intel about Russia's Interference in US-Elections," *deVolkskant*, January 25, 2018, https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/.

357 Ellen Nakashima and Craig Timberg, "Russian Government Hackers are Behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce," *Washington Post*, December 14, 2020, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

358 Adam Meyers, "Meet CrowdStrike's Adversary of the Month for March: VENOMOUS BEAR," *CrowdStrike*, March 12, 2018, https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/; Osborne, "Russian APT Turla Targets 35 Countries."

359 Andy Greenberg, "Your Guide to Russia's Infrastructure Hacking Teams," *Wired*, July 12, 2017, https://www.wired.com/story/russian-hacking-teams-infrastructure/.

360 Defense Security and Counterintelligence Agency, *Targeting U.S. Technologies*, 5.

361 Defense Security and Counterintelligence Agency, *Targeting U.S. Technologies*, 7, 9.

362 Bundesamt für Verfassungsshutz, "Hinweis auf aktuelle Angriffskampagne" ("Report on Current Attack Campaign"), Cyber-Brief Nr. 01/2016, March 3, 2016, 2, https://www.verfassungsschutz.de/embed/broschuere-2016-03-bfv-cyber-brief-2016-01.pdf.

363 Chris Fox and Leo Kelion, "Coronavirus: Russian Spies Target Covid-19 Vaccine Research," *BBC News*, July 16, 2020, https://www.bbc.com/news/technology-53429506.

364 National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*, 14.

365 National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*, 8.

366 Belousova posted her resume online in about 2007 to https://www.weblancer.net/users/eas7/. Her personal website is http://eas7.ru/, which was active in 2009-11.

367 Vice TV Twitter Feed, December 6, 2016.

368 Patrick Reevell, "How Russia Is Using Facial Recognition To Police Its Coronavirus Lockdown," *ABC News*, April 30, 2020, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736; "Russia To Install 'Orwell' Facial Recognition Tech in Every School," *Moscow Times*, June 16, 2020, https://www.themoscowtimes.com/2020/06/16/russia-to-install-orwell-facial-recognition-tech-in-every-school-vedomosti-a70585; Anna Baydakova, "Facial Recognition Tech May Be Being Used Against Russian Protestors," *Coindesk*, February 1, 2021, https://www.yahoo.com/finance/news/facial-recognition-tech-may-being-213701268.html.

369 Corera, *Russians Among Us*, 81-82; Mark Urban, *The Skripal Files* (London: Pan Books, 2019).

370 Pavel Felgenhauer, "Russia's Imperial General Staff," *Perspective* XVI, no. 1 (October-November 2005): www.bu.ed./iscip/vol16/felgenhauer.

371 Main Intelligence Directorate (GRU) of the Soviet Armed Forces General Staff, Moscow to Ottawa, GRU Telegram number 11273, dated August 11, 1945, The National Archives, Kew, London, KV 2/1427, item number 98; British Embassy in New York to Foreign Office, Telegram dated September 10, 1945, The National Archives, KV 2/1419, serial 3a.

372 MI6, "The Corby Case," Secret Intelligence Service Summary of Gouzenko Interrogations, The National Archives, Kew, London, KV 2/1420, 17.

373 See, for example, General Valery Gerasimov, "Ценность науки в предвидении: Новые вызовы требуют переосмыслить формы и способы ведения боевых действий" ["The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations"] *Voyenno-Promyshlennyy Kurier*, February 26, 2013, http://vpk-news.ru/articles/14632.

374 Michael Kofman, "Russian Performance in the Russo-Georgian War Revisited," *War on the Rocks*, September 4, 2018, https://warontherocks.com/2018/09/russian-performance-in-the-russo-georgian-war-revisited/.

375 "Georgia Says Russian Hackers Block Govt Websites," *Reuters*, August 11, 2008, https://uk.reuters.com/article/us-georgia-ossetia-hackers/georgia-says-russian-hackers-block-govt-websites-idUKLB2050320080811.

376 Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, DC: Georgetown University Press, 2020), 36-40.

377 "Georgia Accuses Russia of Widespread Cyber Attack," Agenda.ge, February 20, 2020, https://agenda.ge/en/news/2020/535; Ryan Browne, "US and UK Accuse Russia of Major

Cyber Attack on Georgia," *CNN*, February 20, 2020, https://www.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html.

378 Scott Neuman, "Ukraine To Expel Russian Diplomat Caught Taking Classified Info," *NPR*, May 1, 2014, https://www.npr.org/sections/thetwo-way/2014/05/01/308605849/ukraine-to-expel-russian-diplomat-caught-taking-classified-info.

379 Matthias Williams, "Russian Diplomats Expelled from Moldova Recruited Fighters–Sources," *Reuters*, June 13, 2017, https://www.reuters.com/article/us-moldova-russia-expulsions/exclusive-russian-diplomats-expelled-from-moldova-recruited-fighters-sources-idUSKBN1941DA.

380 Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 18, 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

381 "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," *CrowdStrike*, March 23, 2017, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

382 Patrick Tucker, "Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says," *Defense One*, December 7, 2018, https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/.

383 Glen E. Howard and Matthew Czekaj, eds., *Russia's Military Strategy and Doctrine* (Washington, DC: The Jamestown Foundation, 2019), 11, 19.

384 Missy Ryan, "Russian, Syrian partnership poses a new challenge for U.S. in Iraq," *Washington Post*, September 28, 2015, https://www.washingtonpost.com/world/national-security/russian-syrian-partnership-poses-a-new-challenge-for-us-in-iraq/2015/09/28/b1190982-65ee-11e5-9223-70cb36460919_story.html.

385 Igor Gouzenko, "I Was Inside Stalin's Spy Ring," *Cosmopolitan*, March 1947.

386 Australian Security Intelligence Organisation Memo, May 12, 1954, National Archives of Australia, A6283, folder 1, item number 4104669, 99; duplicate in National Archives of Australia, A6283, folder 14, item number 4104675, 34. The U.S. VENONA decryption program had identified the code word ENORMOZ at least by the late 1940s as referring to the U.S. Manhattan Project. Kartseva remembered the same code word as describing the equivalent Australian program.

387 Andrew and Mitrokhin, *The Sword and the Shield*, 447-48.

388 Andrew and Gordievsky, *Comrade Kryuchkov's Instructions*, 18.

389 Andrew and Mitrokhin, *The Sword and the Shield*, 392-93.

390 Andrew and Mitrokhin, *The Sword and the Shield*, 214.

391 Booz Allen Hamilton, *Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations* (McLean, VA: Booz Allen Hamilton, 2020), 15.

392 Ministry of Foreign Affairs of the Russian Federation, *Foreign Policy Concept*, 21.

393 Ministry of Foreign Affairs of the Russian Federation, *Foreign Policy Concept*, 9.

394 Lesley Kucharski, *Russian Multi-Domain Strategy Against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe* (Livermore, CA: Lawrence Livermore National Laboratory, 2018), 23.

395 Dave Johnson, *Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds*, Livermore Papers on Global Security No. 3, Lawrence Livermore National Laboratory, Center for Global Security Research, February 2018, 52-54; Michael Kofman, Anya Fink, Jeffrey Edmonds, *Russian Strategy for Escalation Management: Evolution of Key Concepts* (Arlington, VA: Center for Naval Analysis, 2020), 61-63.

396 Russian Federation, "О внесении изменений в Федеральный закон 'О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера'" ["Amendments to the Federal Law 'On the Defense of the Population and Territory from Extreme Natural or Technological Situations'"], Federal Law No. 38-F3, March 8, 2015, http://base.garant.ru/70885212/#ixzz6eHSZ0hDq.

397 Andrew and Mitrokhin, *The Sword and the Shield*, 360-61.

398 "Defection of KGB Officer," September 16, 1971, British government document contained in FBI file number 105-216642, serial 7, received by FOIA.

399 Kalugin, *Spymaster*, 147.

400 Andrew and Mitrokhin, *The World Was Going Our Way*, 173-74.

401 Security Service of Ukraine, "SSU Successfully Counteracts Hacker Attacks of Russian Special Services," Press Release, March 13, 2015, http://www.sbu.gov.ua/sbu/control/en/publish/article?art_id=138949&cat_id=35317.

402 Cybersecurity and Infrastructure Security Agency (CISA), "ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure," February 25, 2016, https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.

403 U.S. Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Press Release, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

404 Adam Meyers, "CrowdStrike's January Adversary of the Month: VOODOO BEAR," *CrowdStrike*, January 29, 2018, https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/; Andy Greenberg, "Your Guide to Russia's Infrastructure Hacking Teams."

405 "CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations," *Dragos*, June 2017, https://dragos.com/wp-content/uploads/CrashOverride-01.pdf; Pavel Polityuk, "Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid," *Reuters,* December 20, 2016, https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF.

406 Pavel Polityuk and Alessandra Prentice, "Ukrainian Banks, Electricity Firm Hit by Fresh Cyber Attack," *Reuters*, June 27, 2017, https://www.reuters.com/article/us-ukraine-cyber-

attacks-idUSKBN19I1IJ; Andrew Griffin, "'Petya' Cyber Attack: Chernobyl's Radiation Monitoring System Hit by Worldwide Hack, Monitoring Is Now Being Performed Manually, Ukrainian Authorities Said," *Independent*, June 27, 2017, https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html; Lizzie Dearden, "Ukraine Cyber Attack: Chaos as National Bank, State Power Provider and Airport Hit by Hackers: Russian Energy Firms and Danish Shipping Company also Hit by Hackers," *Independent*, June 27, 2017, https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html.

407 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

408 John Leyden, "Ukraine Claims It Blocked VPNFilter Attack at Chemical Plant," theregister.co.uk, July 13, 2018, https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/; "SBU Thwarts Cyber Attack from Russia Against Chlorine Station in Dnipropetrovsk Region," *Interfax-Ukraine*, July 11, 2018, https://en.interfax.com.ua/news/general/517337.html.

409 Andy Greenberg, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," *Wired*, October 17, 2019, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

410 Cybersecurity and Infrastructure Security Agency, "Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors," originally published October 20, 2017, updated March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA17-293A; Jim Finkle, "U.S. Warns Businesses Of Hacking Campaign against Nuclear, Energy Firms," *Reuters*, June 30, 2017, https://www.reuters.com/article/us-usa-cyber-energy/u-s-warns-businesses-of-hacking-campaign-against-nuclear-energy-firms-idUSKBN19L2Z9; Pete Williams, "Russian Hackers Targeted Control Systems for Electric Utilities, Homeland Security Says," *NBC News*, July 24, 2018, https://www.nbcnews.com/politics/politics-news/russian-hackers-targeted-control-systems-electric-utilities-homeland-security-says-n894226; "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *Wall Street Journal*, July 23, 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110.

411 Nicole Perlroth, "Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid," *New York Times*, October 24, 2020, https://www.nytimes.com/2020/10/23/us/politics/energetic-bear-russian-hackers.html.

412 Bundesamt für Verfassungsshutz, "Hinweis auf aktuelle Angriffskampagne" ["Report on Current Attack Campaign"], Cyber-Brief Nr. 01/2018, June 7, 2018, https://www.verfassungsschutz.de/embed/broschuere-2018-06-bfv-cyber-brief-2018-01-neu.pdf; Andrea Shalal, "German Intelligence Sees Russia Behind Hack of Energy Firms: Media

Report," *Reuters*, June 20, 2018, https://www.reuters.com/article/us-germany-cyber-russia/german-intelligence-sees-russia-behind-hack-of-energy-firms-media-report-idUSKBN1JG2X2; Catalin Cimpanu, "Two More Cyber-attacks Hit Israel's Water System," *Zero Day*, July 20, 2020, https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/.

413 Dorfman, "The Secret History of the Russian Consulate in San Francisco."

414 John Mooney, "Russian Agents Plunge to New Ocean Depths in Ireland To Crack Transatlantic Cables," *Sunday Times*, February 16, 2020, https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz.

415 Peter Cooney, "U.S. Concerned by Russian Operations Near Undersea Cables: NY Times," *Reuters*, October 25, 2015, https://www.reuters.com/article/us-usa-security-russia/u-s-concerned-by-russian-operations-near-undersea-cables-ny-times-idUSKCN0SK02G20151026.

416 Steffan Watkins, "We Will Bury You (in Data)—Russian Navy Yantar Backgrounder and Summer 2016 Trip Report," vesselofinterst.com, November 3, 2018, https://www.vesselofinterest.com/2018/11/we-will-bury-you-in-data-russian-navy.html.

417 Andrew Chuter, "Russia's Naval Updates Threaten Undersea Comms Network, Says Top British Military Officer," *DefenseNews*, December 15, 2017, https://www.defensenews.com/naval/2017/12/15/russias-naval-updates-threaten-undersea-comms-network-says-top-british-military-officer/.

418 Gregory Hinck, "Evaluating the Russian Threat to Undersea Cables," Lawfare Blog, March 5, 2018, https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

419 Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview: Irreversible Implementation of the National Defense Strategy, United States Department of Defense Fiscal Year 2021 Budget Request* (Washington, DC: Department of Defense, February 2020).

420 Ukrtelekom, "Укртелеком офіційно повідомляють про блокування невідомими декількох вузлів зв'язку на півострові" ["Ukrtelekom officially reports blocking of communications nodes on peninsula by unknown actors"], Press Release, February 28, 2014, http://www.ukrtelecom.ua/presscenter/news/official?id=120327, cited in Keir Giles, "Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power" (London: Chatham House Russia and Eurasia Programme, March 2016), 64.

421 Mitrokhin, ed., *KGB Lexicon*.

422 Yevgeniy Primakov, "Разведка в современном мире" ["Intelligence in the Modern World"], speech given to the Journalism Faculty, Moscow State University, October 14, 1992, in Yevgeniy Primakov (ed.), *Очерки истории российской внешней разведки* [*Essays on the History of Russian Foreign Intelligence*], vol. 6 (Moscow: Mezdunarodniya Otnosheniya, 2014), 213.

423 U.S. Congress. Senate. Select Committee on Intelligence, *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*, Testimony of Thomas Rid, 115th Congress, March 30, 2017, 2, https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf.

424 U.S. Congress. Senate. Select Committee on Intelligence, *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*, 1.

425 U.S. Department of State, Bureau of Public Affairs, *Soviet "Active Measures": Forgery, Disinformation, Political Operations*, Special Report No. 88, October 1981, 4.

426 U.S. Department of State, *Soviet "Active Measures": Forgery, Disinformation, Political Operations*.

427 U.S. Department of State, *Soviet "Active Measures": Forgery, Disinformation, Political Operations*, 4.

428 Thomas Boghardt, "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence* 53, no. 4 (December 2009): 1-24.

429 Todd Leventhal, "Traffic in Baby Parts Has No Factual Basis," *New York Times*, February 26, 1992.

430 See, for example, the Russian-manufactured false report claiming CIA involvement in the MH17 shoot down in Caleb Gilbert (pseudo), "David L. Stern's Phone Talks before Malaysian Airlines 17 Plane Crash," pressbox.co.uk, July 17, 2015.

431 Rikard Jozwiak, "EU Lawmakers Say Russia Using Coronavirus Crisis for Political Benefit," *RFE/RL*, April 3, 2020, https://www.rferl.org/a/eu-lawmakers-say-russia-using-coronavirus-crisis-to-gain-political-benefits/30529085.html.

432 John B. Emerson, "Exposing Russian Disinformation," *Atlantic Council UkraineAlert*, June 29, 2015, https://www.atlanticcouncil.org/blogs/ukrainealert/exposing-russian-disinformation/.

433 Leonid Bershidsky, "Putin's Latest Obsession: A New World War II Narrative," *Bloomberg*, January 10, 2020, https://www.bloomberg.com/opinion/articles/2020-01-10/putin-s-latest-obsession-rewriting-world-war-ii.

434 Ben Nimmo, "How MH17 Gave Birth to the Modern Russian Spin Machine," *Foreign Policy*, September 29, 2016, https://foreignpolicy.com/2016/09/29/how-mh17-gave-birth-to-the-modern-russian-spin-machine-putin-ukraine/.

435 "Russian Hackers Leak Simone Biles and Serena Williams Files," *BBC*, September 13, 2016, https://www.bbc.com/news/world-37352326.

436 Karoun Demirjian, "Putin Denies Russian Troops Are in Ukraine, Decrees Certain Deaths Secret," *Washington Post*, May 28, 2015, https://www.washingtonpost.com/world/putin-denies-russian-troops-are-in-ukraine-decrees-certain-deaths-secret/2015/05/28/9bb15092-0543-11e5-93f4-f24d4af7f97d_story.html; Carl Schreck, "From 'Not Us' To 'Why Hide It'?: How Russia Denied Its Crimea Invasion, Then Admitted It," *Radio Free Europe/Radio Liberty*, February 26, 2019, https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html.

437 Andrew Roth, "Vladimir Putin Calls Sergei Skripal a Scumbag and a Traitor," *Guardian*, October 3, 2018, https://www.theguardian.com/uk-news/2018/oct/03/vladimir-putin-calls-sergei-skripal-a-scumbag-and-traitor.

438 Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

439 Rid, *Active Measures*, 377-96.

440 "The Dreadful Eight: GRU's Unit 29155 and the 2015 Poisoning of Emilian Gebrev," *Bellingcat*, November 23, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/11/23/the-dreadful-eight-grus-unit-29155-and-the-2015-poisoning-of-emilian-gebrev/.

441 "Remarks of Aleksandr Yurievich Kaznacheyev before the Overseas Press Club, New York City," December 17, 1959, 4, CIA FOIA Reading Room.

442 Gilbert (pseudo), "David L. Stern's Phone Talks before Malaysia Airlines Flight 17 Plane Crash."

443 U.S. Department of Justice, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations."

444 U.S. Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace"; Andy Greenberg, "Here's the Evidence That Links Russia's Most Brazen Cyberattacks," *Wired*, November 15, 2019, https://www.wired.com/story/sandworm-russia-cyberattack-links/; Greenberg, "The Untold Story of the 2018 Olympics Cyberattack."

445 U.S. Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," Press Release, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0126.

446 Anton Troianovski, Ellen Nakashima, and Shane Harris, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West," *Washington Post*, December 28, 2018, https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

447 Mitch Prothero, "'Unit 29155': Putin's Assassination Squad—Suspected of Killings All Over Europe—Received Diplomatic Cover from the Russian Mission in Switzerland," *Business Insider*, March 16, 2020, https://www.businessinsider.com/unit-29155-assassination-squad-diplomatic-russia-mission-switzerland-2020-3; "An Officer and A Diplomat: The Strange Case of the GRU Spy With a Red Notice," *Bellingcat*, February 25, 2020, https://www.bellingcat.com/news/2020/02/25/an-officer-and-a-diplomat-the-strange-case-of-the-gru-spy-with-a-red-notice/.

448 Viktor Suvorov, *Inside Soviet Military Intelligence* (New York: MacMillan, 1984); Viktor Suvorov, *Spetsnaz: The Inside Story of the Soviet Special Forces* (New York; London: Norton, 1988); Suvorov, *Aquarium: The Career and Defection of a Soviet Military Spy*.

449 Boris Egorov, "5 Legendary Russian Special Forces Units," *Russia Beyond*, November 30, 2018, https://www.rbth.com/science-and-tech/329610-5-legendary-russian-special-forces.

450 Steven Rosenberg, "Ukraine Crisis: Meeting the Little Green Men," *BBC*, April 30, 2014, https://www.bbc.com/news/world-europe-27231649.

451 Schreck, "From 'Not Us' To 'Why Hide It?'"

452 Neil Hauer, "Russia's Favorite Mercenaries: Wagner, the Elusive Private Military Company, Has Made Its Way to Africa—with Plenty of Willing Young Russian Volunteers," *The Atlantic*, August 27, 2018, https://www.theatlantic.com/international/archive/2018/08/russian-mercenaries-wagner-africa/568435/.

453 Pierre Vaux, "Fontanka Investigates Russian Mercenaries Dying for Putin in Syria and Ukraine," *The Interpreter*, March 29, 2016, https://www.interpretermag.com/fontanka-investigates-russian-mercenaries-dying-for-putin-in-syria-and-ukraine/.

454 Thomas Gibbons-Neff, "How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html.

455 Pjotr Sauer, "In Push for Africa, Russia's Wagner Mercenaries Are 'Out of Their Depth' in Mozambique," *The Moscow Times*, November 19, 2019, https://www.themoscowtimes.com/2019/11/19/in-push-for-africa-russias-wagner-mercenaries-are-out-of-their-depth-in-mozambique-a68220; Daniel Sixto, "Russian Mercenaries: A String of Failures in Africa," *Geopolitical Monitor*, August 24, 2020, https://www.geopoliticalmonitor.com/russian-mercenaries-a-string-of-failures-in-africa/.

456 "Berlin Murder: Germany Expels two Russian Diplomats," *BBC*, December 4, 2019, https://www.bbc.com/news/world-europe-50659179.

457 "Alexei Navalny: Putin Critic Arrives in Germany for Medical Treatment," *BBC*, August 22, 2020, https://www.bbc.com/news/world-europe-53871617.

458 "Gas 'Killed Moscow Hostages,'" *BBC*, October 27, 2002, http://news.bbc.co.uk/2/hi/europe/2365383.stm; "Timeline: The Beslan School Siege," *Guardian*, September 6, 2004, https://www.theguardian.com/world/2004/sep/06/schoolsworldwide.chechnya.

459 Mike Eckel, "Two Decades On, Smoldering Questions About The Russian President's Vault To Power," *Radio Free Europe/Radio Liberty*, August 7, 2019, https://www.rferl.org/a/putin-russia-president-1999-chechnya-apartment-bombings/30097551.html.

460 Steven Eke, "Russia Law on Killing 'Extremists' Abroad," *BBC*, November 27, 2006, http://news.bbc.co.uk/2/hi/europe/6188658.stm.

461 Russian Federation, "On Countering Terrorism," Article 22, "Lawful Causing of Harm," Federal Law No. 35-F3, June 3, 2006, available at http://www.consultant.ru/document/cons_doc_LAW_58840/.

462 Nathan Hodge, Emma Burrows, and Tara John, "Putin: Sergei Skripal Is a Scumbag and Traitor Who Betrayed Russia," *CNN*, October 4, 2018, https://www.cnn.com/2018/10/03/europe/putin-calls-skripal-scumbag-intl.

463 Christopher Nehring, "Umbrella or Pen? The Murder of Georgi Markov. New Facts and Old Questions," *Journal of Intelligence History* 16, no. 1 (November 22, 2016): 47-58, https://www.tandfonline.com/doi/full/10.1080/16161262.2016.1258248.

464 Cobain, "Boris Berezovsky Inquest Returns Open Verdict on Death."

465 J.J. Green, "Assassins Inc.: The Kremlin's Secret Squad of Killers," WTOP.com, October 22, 2018, https://wtop.com/j-j-green-national/2018/10/assassins-inc-the-kremlins-secret-squad-of-killers/.

466 Michael Schwirtz, "Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say," *New York Times*, October 8, 2019, https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html.

467 "Montenegro Jails 'Russian Coup Plot' Leaders," *BBC*, May 9, 2019, https://www.bbc.com/news/world-europe-48212435.

468 U.S. Army, Counterintelligence Corps File, "Hans Kukowitsch," National Archives and Records Administration, RG 319, Entry A1 314B, Box 443. Kukowitsch was Khokhlov's assistant in the Okolovich operation. Serhii Plokhy, *The Man with the Poison Gun* (London: Oneworld, 2016).

469 Loveday Morris, Ladka Bauerova, and Robyn Dixon, "Accusations of Spying and Sabotage Plunge Russian-Czech Relations into the Deep Freeze," *Washington Post*, April 19, 2021, https://www.washingtonpost.com/world/europe/russia-diplomats-expulsions-czech/2021/04/19/ef7f6178-9fbb-11eb-b2f5-7d2f0182750d_story.html.

470 "Emilian Gebrev Assassination Attempt Investigation, 2015," *Bellingcat*, September 4, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/09/04/gebrev-survives-poisonings-post-mortem/.

471 Mike Eckel, Ivan Bedrov, Olha Komarova, "A Czech Explosion, Russian Agents, a Bulgarian Arms Dealer: The Recipe for a Major Spy Scandal in Central Europe," *Radio Free Europe/Radio Liberty*, April 18, 2021, https://www.rferl.org/a/czech-expulsions-bulgaria-gebrev-russia-gru-intelligence-explosion-spy-scandal/31209960.html.

472 Loveday Morris and Robyn Dixon, "Bulgaria Alleges Russian Links to Arms Depot Blasts, Widening European Probes into Moscow Agents," *Washington Post*, April 28, 2021, https://www.washingtonpost.com/world/europe/bulgaria-russia-arms-explosions-czech-republic/2021/04/28/ba2e7004-a812-11eb-a8a7-5f45ddcdf364_story.html.

473 O. S. Smyslov, *Генерал Абакумов. Палач или жертва?* [*General Abakumov: Executioner or Victim*] (Moscow: Veche, 2012), http://www.e-reading.me/chapter.php/1015673/54/Smyslov_-_General_Abakumov._Palach_ili_zhertva.html.

474 Kalugin, *Spymaster*, 108.

475 Andrew and Mitrokhin, *The Sword and the Shield*, 149.

476 Richard Cummings, *Cold War Radio: The Dangerous History of American Broadcasting in Europe, 1950-1989* (Jefferson, NC: McFarland and Co., 2009), 176-78; *Разведчики Разоблачают... Эта Кинга о Шпионской и Подрывной Деятельности Радиостанций*

"Свобода" и "Свободная Европа" [*Intelligence Officers Reveal... This Book Is About the Espionage and Underground Activity of the Radio Stations "Liberty" and "Free Europe"*] (Moscow: Molodaya Gvardiya, 1977).

477 Kalugin, *Spymaster*, 275.

478 "Alexander Litvinenko: Profile of Murdered Russian Spy," *BBC*, January 21, 2016, https://www.bbc.com/news/uk-19647226.

479 James Masters, "Theresa May's Full Statement on Russian Spy's Poisoning," *CNN*, March 13, 2018, https://www.cnn.com/2018/03/13/europe/theresa-may-russia-spy-speech-intl/index.html; "Skripal Suspect Boshirov Identified as GRU Colonel Anatoliy Chepiga," *Bellingcat*, September 26, 2018, https://www.bellingcat.com/news/uk-and-europe/2018/09/26/skripal-suspect-boshirov-identified-gru-colonel-anatoliy-chepiga/; "Full Report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia," *Bellingcat*, October 9, 2018, https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/.

480 "Семья шпиона Смоленкова сбежала из своего дома в США" ["The Family of Spy Smolenkov Disappeared from their Home in the USA"], Lenta.ru, September 11, 2019, https://lenta.ru/news/2019/09/11/runaway/.

481 Siegfried Mortkowitz, "Czechs Expel More Russian Embassy Staff Over Bombing Claims," *Politico*, April 22, 2021, https://www.politico.eu/article/czech-republic-russia-embassy-staff-bombing-claims/.

482 Australian Security Intelligence Organisation Investigative Memo, April 13, 1953, National Archives of Australia (NAA), A6117, folder 8, item number 12077929, serial 154; "Statement by Petrova," October 14, 1954, NAA, A6283, folder 15, item number 4104676, 80; "Moscow Instructions to Canberra," January 2, 1952, NAA, A6283, folder 1, item number 4104669, 1-2.

483 Earley, *Comrade J*, 224-68.

484 Vladimir Vanin, "Ай да мы: взяли русского Джеймса Бонда!" ["Oh My: A Russian James Bond Is Arrested!"], *Nezavisimoe Voennoe Obozrenie*, January 22, 2010.

485 U.S. Magistrate Judge, Southern District of New York, "USA v. Evgeny Buryakov et al."

486 "Сергей Нарышкин: нелегалы—золотой фонд внешней разведки" ["Sergey Naryshkin: Illegals Are the Golden Reserve of Foreign Intelligence"], *TASS*, June 27, 2017, https://tass.ru/interviews/4366965.

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

488 *Personal History of Hede Massing*, Hoover Institution Archive, Hede Massing Papers, Box 1, Folder 1, 15-17.

489 Bronnikov and Vavilova, *The Woman Who Knows How to Keep Secrets.*

490 Corera, *Russians Among Us*, 209-12.

491 "'Штучные люди': СВР рассекретила выдающихся разведчиков-нелегалов" ["'Extraordinary People': The SVR Declassified Outstanding Illegal Intelligence Officers"], *RIA Novosti*, January 28, 2020, https://ria.ru/20200128/1563982674.html.

492 "Путин рассказал, что его работа в КГБ была связана с нелегальной разведкой" ["Putin Related that His Work in the KGB Was Connected to Illegal Intelligence"], *RIA Novosti*, June 6, 2017, https://ria.ru/20170624/1497218985.html?in=t.

493 Krutikov, "Russian Illegal Intelligence Remains an Object of Envy in the West."

494 Corera, *Russians Among Us*.

495 Nikolay Dolgopolov, "В разведку на всю жизнь" ["Into Intelligence for Life"], *Rossiyskaya Gazeta*, December 20, 2020, https://rg.ru/2020/03/24/istoriia-razvedchika-mihaila-vasenkova-rassekrechennogo-v-2020-godu.html.

496 U.S. Department of Justice, Southern District of New York, "USA vs. Anna Chapman and Mikhail Semenko," June 27, 2010, 3, https://www.justice.gov/sites/default/files/opa/legacy/2010/06/28/062810complaint1.pdf.

497 Pierre Briançon, "The Spanish Story of a Russian 'Illegal,'" *Politico*, June 16, 2016, https://www.politico.eu/interactive/the-spanish-story-of-a-russian-illegal-russian-spy-moscow/.

498 Corera, *Russians Among Us*, 325.

499 Corera, *Russians Among Us*, 307.

500 Bronnikov and Vavilova, *The Woman Who Knows How to Keep Secrets*, Chapter 30.

501 Corera, *Russians Among Us*, 212.

502 Vincent Jauvert, "Révélations sur les espions russes en France" ["Revelations about Russian Spies in France"], L'Obs.com, July 24, 2014.

503 U.S. Army, 441st Counterintelligence Corps (CIC) Detachment Investigative Summary, "REILLY, James Arthur," March 13, 1945, National Archives and Records Administration, RG 319, Entry A1 314B, Box 627.

504 Suvorov, *Aquarium: The Career and Defection of a Soviet Military Spy*, 139-58.

505 Lewis, "Russian Spy Targeted MPs and Whitehall Officials."

506 Alexander Kaznacheev, *Inside a Soviet Embassy* (New York: Lippincott, 1962).

507 Arkady N. Shevchenko, *Breaking with Moscow* (New York: Knopf, 1985).

508 Canadian Broadcasting Corporation, "The KGB Connections."

509 Krasnov, *Soviet Defectors*.

510 Oleg Tumanov, *Tumanov: Confessions of a KGB Agent* (Chicago, IL: Edition Q, 1994).

511 Desmond Ball, *Soviet Signals Intelligence (SIGINT)* (Canberra: Australian National University, 1989), 3-4.

512 Victor Sheymov, *Tower of Secrets: A Real Life Spy Thriller* (Annapolis, MD: Naval Institute Press, 1993), 419.

513 John Prados, "The Navy's Biggest Betrayal," *Naval History Magazine* 24, no. 3 (June 2010), https://www.usni.org/magazines/naval-history-magazine/2010/june/navys-biggest-betrayal.

514 Frank J. Rafalko, ed., *CI Reader: American Revolution Into the New Millennium*, vol. 3, (Washington, DC: Office of the National Counterintelligence Executive, 2004), 409; Jürgen Dahlkamp, "No Country More Beautiful," *New York Times*, July 14, 2003, https://www.nytimes.com/2003/07/14/international/europe/no-country-more-beautiful.html.

515 Lezina, "Dismantling the State Security Apparatus," 4, 8.

516 "ФСО" ("FSO"), *Voenpro*, October 22, 2013, https://voenpro.ru/infolenta/fco.

517 Rostec, "Ростех презентует станцию радиотехнической разведки ПОСТ-3М" ("Rostec Presents the POST-3M SIGINT Station"), Press Release, June 24, 2019, https://rostec.ru/news/rostekh-prezentuet-stantsiyu-radiotekhnicheskoy-razvedki-post-3m/.

518 Ball, *Soviet Signals Intelligence (SIGINT)*, 26.

519 U.S. Departments of State and Defense, *The Soviet-Cuban Connection in Central America and the Caribbean* (Washington, DC: U.S. Departments of State and Defense, 1985), 4.

520 Aleksandr Kolpakidi, *Империя ГРУ* (*The GRU Empire*) (Moscow: Olma-Press, 1999), https://www.litmir.me/br/?b=107721.

521 Victor Robert Lee, "Satellite Images: A (Worrying) Cuban Mystery," *The Diplomat*, June 8, 2018, https://thediplomat.com/2018/06/satellite-images-a-worrying-cuban-mystery/; "Russian Official: We Are Working on Reopening Cuba, Vietnam Bases," Voice of America, October 7, 2016, https://www.voanews.com/europe/russian-official-we-are-working-reopening-cuba-vietnam-bases.

522 Keir Giles, *Russian Ballistic Missile Defense: Rhetoric and Reality* (Carlisle, PA: U.S. Army War College, 2015), 13-14; "Увидеть футбольный мяч с 8000 км: как устроена ПВО России" ["To See a Football from 8,000 km: That is How the PVO of Russia Works"], *TVZvezda*, May 17, 2015; "Russian Long-range Radar in Belarus To Track U.S. Missile Defense System in Europe," Belta.by, February 15, 2012, https://eng.belta.by/society/view/russian-long-range-radar-in-belarus-to-track-us-missile-defense-system-in-europe-137481-2021/.

523 "Russia's Decision To Close Down Gabala Radar Station Is Final–Lavrov," *Interfax*, January 23, 2013, https://www.rbth.com/news/2013/01/23/russias_decision_to_close_down_gabala_radar_station_is_final_-_lavrov_pa_22129.html.

524 "'Окно' в Таджикистане 'увидит' объекты в космосе на расстоянии 50 тысяч км" ["The 'Okno' in Tajikistan 'Sees' Objects in Space at a Distance of 50 Thousand km"], *RIA Novosti*, November 27, 2016, https://news.rambler.ru/science/35393642-okno-v-tadzhikistane-uvidit-obekty-v-kosmose-na-rasstoyanii-50-tysyach-km/.

525 Estonian Foreign Intelligence Service, "How the FSB Signal Intelligence Gathers Information on Foreign Citizens," in *International Security and Estonia 2019* (Tallinn, Estonia: Välisluureamet, 2019), 54-58.

526 Ball, *Soviet Signals Intelligence (SIGINT)*, 38.

527 Andrew and Mitrokhin, *The Sword and the Shield*, 343.

528 Kalugin, *Spymaster*, 102.

529 Dorfman, "The Secret History of the Russian Consulate in San Francisco."

530 Canadian Broadcasting Corporation, "The KGB Connections."

531 Missy Ryan, Ellen Nakashima, and Karen DeYoung, "Obama Administration Announces Measures To Punish Russia for 2016 Election Interference," *Washington Post*, December 29, 2016, https://www.washingtonpost.com/world/national-security/obama-administration-announces-measures-to-punish-russia-for-2016-election-interference/2016/12/29/311db9d6-cdde-11e6-a87f-b917067331bb_story.html.

532 William Safire, "Who Lost Mount Alto," *New York Times*, September 22, 1985; Canadian Broadcasting Corporation, "The KGB Connections."

533 Canadian Broadcasting Corporation, "The KGB Connections."

534 Kalugin, *Spymaster*, 102.

535 Ball, *Soviet Signals Intelligence (SIGINT)*, 43.

536 Nigel West, *Historical Dictionary of Signals Intelligence* (Lanham, MD: Scarecrow Press, 2012), 126, 251.

537 Andrew and Mitrokhin, *The Sword and the Shield*, 349.

538 Earley, *Comrade J*, 255-59.

539 Zach Dorfman, Jenna McLaughlin, and Sean D. Naylor, "Russia Carried Out a 'Stunning' Breach of FBI Communications System, Escalating the Spy Game on U.S. Soil," *Yahoo News*, September 16, 2019, https://news.yahoo.com/exclusive-russia-carried-out-a-stunning-breach-of-fbi-communications-system-escalating-the-spy-game-on-us-soil-090024212.html.

540 "Dutch Government Says It Disrupted Russian Attempt To Hack Chemical Weapons Watchdog."

541 "How the Dutch Foiled Russian 'Cyber-Attack' on OPCW," *BBC*, October 4, 2018, https://www.bbc.com/news/world-europe-45747472#share-tools. Although the media referred to this incident as a "cyber-attack," it was most likely a close access SIGINT operation.

542 Olsen, "Norway Says Russia Was Behind Hacker Attack on Parliament."

543 Emma Tucker, "Swiss Police Suspect Russian Spies Posed as Plumbers to Surveil Davos: Report," *Daily Beast*, January 21, 2020, https://www.thedailybeast.com/swiss-police-suspect-russian-spies-posed-as-plumbers-to-surveil-davos-report-says.

544 Ali Watkins, "Russia Escalates Spy Games After Years of U.S. Neglect," *Politico*, June 1, 2017, https://www.politico.com/story/2017/06/01/russia-spies-espionage-trump-239003; Dorfman, "The Secret History of the Russian Consulate in San Francisco."

545 Cummings, *Cold War Radio*, 176-77.

546 Ball, *Soviet Signals Intelligence (SIGINT)*, 95-107.

547 Sam LaGrone, "Coast Guard: Russian Surveillance Ship Operating in 'Unsafe' Manner off East Coast," *USNI News*, December 17, 2019, https://news.usni.org/2019/12/17/coast-guard-russian-surveillance-ship-operating-in-unsafe-manner-of-east-coast.

548 "On the Horizon: Navigating the European and African Theaters—Episode 14," interview with Admiral James Foggo, Commander of U.S. Naval Forces Europe, Commander Sixth Fleet Public Affairs, December 6, 2019, https://www.c6f.navy.mil/Media/transcripts/

Article/2043849/on-the-horizon-navigating-the-european-and-african-theaters-episode-14/.

549 Mallory Shelbourne, "No Russian or Chinese Presence at First Week of RIMPAC," *USNI News*, August 24, 2020, https://news.usni.org/2020/08/24/no-russian-or-chinese-presence-at-first-week-of-rimpac.

550 "Russia's Ships, Missile Systems Put on Duty Due to NATO Exercise in Black Sea," *TASS*, April 8, 2019, https://tass.com/defense/1052558.

551 Dan Mcquade, "Russian Spy Ship Spotted Off Coast of Delaware," Phillymag.com, February 14, 2017, https://www.phillymag.com/news/2017/02/14/russian-spy-ship-delaware-coast/.

552 "Full Analysis of the Sinking of Liman," *Plansandstuff*, May 29, 2017, https://planesandstuff.wordpress.com/2017/05/29/full-analysis-of-the-sinking-of-liman/.

553 Cooney, "U.S. Concerned by Russian Operations Near Undersea Cables;" Mooney, "Russian Agents Plunge to New Ocean Depths in Ireland to Crack Transatlantic Cables."

554 Joseph Trevithick, "Russia's Electronic Spies Are Hard at Work in Syria: Signal Spooks Search for Targets and Follow up on Strikes," Warisboring.com, October 7, 2015, https://warisboring.com/russias-electronic-spies-are-hard-at-work-in-syria/; Seth Jones, ed., *Moscow's War in Syria* (Washington, DC: Center for Strategic and International Studies, 2020), 20-22.

555 David Cenciotti, "Russia's Most Advanced Spyplane Has Deployed to Syria Again," *Business Insider*, August 1, 2016, https://www.businessinsider.com/russias-most-advanced-spyplane-has-deployed-to-syria-again-2016-8.

556 David Cenciotti, "After the First Tour of Duty in February 2016, the Tu-214R Has Returned to Latakia. To Spy on Daesh (and also on the U.S. F-22s?)," *The Aviationist*, July 31, 2016, https://theaviationist.com/2016/07/31/russias-most-advanced-spyplane-has-deployed-to-syria-again/.

557 "Electronic Weapons: Yet Another New Russian EW Aircraft," *Strategy Page*, August 28, 2017, https://www.strategypage.com/htmw/htecm/articles/20170818.aspx.

558 "How Russia Air Force Jammed Turkish F-16 Aircraft Fighter Jets over Idlib, Syria," *Eurasian Times*, March 9, 2020, https://eurasiantimes.com/how-russian-air-force-jammed-turkish-f-16-fighter-jets-over-idlib-syria/.

559 Jones, ed., *Moscow's War in Syria*, 67-68.

560 "Russia Blames Israel After Military Plane Shot Down off Syria," *BBC*, September 18, 2018, https://www.bbc.com/news/world-europe-45556290.

561 Thomas Nilsen, "Video: Norway's New F-35 Filmed From Russian Anti-submarine Plane," *Barents Observer*, March 10, 2020, https://thebarentsobserver.com/en/security/2020/03/video-norways-new-f-35-filmed-russian-anti-submarine-plane.

562 Ball, *Soviet Signals Intelligence (SIGINT)*, 117-18.

563 Bart Hendrickx, "Snooping on Radars: A History of Soviet/Russian Global Signals Intelligence Satellites," *Space Chronicle, Journal of the British Interplanetary Society* 58, Supplement 1 (2005).

564 Anatoly Zak, "Lotos-S Spacecraft for the Liana system," *Russian Space Web*, October 25, 2018, http://www.russianspaceweb.com/images/spacecraft/military/elint/liana/lotos_m_silo_1.jpg.

565 Anatoly Zak, "US-A and US-P Military Satellites," *Russian Space Web*, last updated January 2, 2020, http://www.russianspaceweb.com/us.html.

566 "Liana Electronic Intelligence Program," SpaceFlight101.com, 2020, http://spaceflight101.com/spacecraft/liana-electronic-intelligence-program/.

567 Stephen Thompson, "History and Historiography of National Security Space," in Stephen Dick and Roger Launius, eds., *Critical Issues in the History of Spaceflight* (Washington, DC: National Aeronautics and Space Administration, 2006), 481-548; Peter Gorin, "Zenit-The First Soviet Photo-Reconnaissance Satellite," *Journal of the British Interplanetary Society* 50 (November 1997): 441-48; Peter Gorin, "Black 'Amber': Russian Yantar-Class Optical Reconnaissance Satellites," *Journal of the British Interplanetary Society* 51 (August 1998), 309-20.

568 Anatoly Zak, "Bars-M: Russia's First Digital Cartographer," *Russian Space Web*, last updated February 5, 2020, http://www.russianspaceweb.com/bars-m.html.

569 Anatoly Zak, "Araks (11F664) Military Spacecraft," *Russian Space Web*, January 3, 2018, http://www.russianspaceweb.com/araks.html.

570 Anatoly Zak, "Persona (14F137) Spy Satellite," *Russian Space Web*, August 29, 2017, http://www.russianspaceweb.com/persona.html.

571 "Kondor Spacecraft Overview," SpaceFlight101.com, 2020, https://spaceflight101.com/spacecraft/kondor/.

572 Anatoly Zak, "US-K and US-KMO Constellations," *Russian Space Web*, last updated November 25, 2019, http://www.russianspaceweb.com/oko.html.

573 Anatoly Zak, "The EKS Kupol Network Design," *Russian Space Web*, last updated December 28, 2019, http://www.russianspaceweb.com/eks-network.html.

574 Kevin Riehle and Michael May, "Human-cyber Nexus: the Parallels Between 'Illegal' Intelligence Operations and Advanced Persistent Threats," *Intelligence and National Security* 34, no. 2 (2018): 189-204, https://www.tandfonline.com/doi/abs/10.1080/02684527.2018.1534642.

575 "Russia's Brain Drain on the Rise over Economic Woes—Report," *The Moscow Times*, January 24, 2018, https://www.themoscowtimes.com/2018/01/24/russias-brain-drain-on-the-rise-over-economic-woes-report-a60263.

576 "Putin Stresses Importance of New Far East Space Center," *RIA Novosti*, August 28, 2010; Matthew Brodner, "The Long Road to Vostochny: Inside Russia's Newest Launch Facility," *Space News*, January 30, 2019, https://spacenews.com/the-long-road-to-vostochny-inside-russias-newest-launch-facility/; Anatoly Zak, "Origin of the Vostochny (formerly Svobodny) Launch Site," *Russian Space Web*, September 8, 2018, http://www.russianspaceweb.com/svobodny.html.

577 Galeotti, *Putin's Hydra*, 14-15.

578 Galeotti, *Putin's Hydra,* 14-15.

579 Riehle, “Assessing Foreign Intelligence Threats.”

580 George W. Bush, “User Clip: Bush Saw Putin's Soul,” CSPAN, June 16, 2001, https://www.c-span.org/video/?c4718091/user-clip-bush-putins-soul.

581 Louise Hall, “Former Russian PM Describes Trump's Presidency as ‘Period of Disappointment,’” *Independent*, February 1, 2021, https://www.independent.co.uk/news/world/americas/us-politics/dmitry-medvedev-trump-presidency-russia-disappointment-b1795684.html.

582 “‘Штучные люди’: СВР рассекретила выдающихся разведчиков-нелегалов” [“‘Extraordinary People’: The SVR Declassified Outstanding Illegal Intelligence Officers”].

583 Yuriy Logvinenko, *История российского шпионажа и сыска глазами филателиста* [*The History of Russian Espionage and Investigation through the Eyes of a Philatelist*] (Moscow: OLMA Media Group, 2012).

584 See, for example, the books of Nikolay Dolgopolov; Kovacevic, “Nikolay Dolgopolov: Storyteller of Soviet Intelligence History.”

585 Andrey Kolesnikov, “ФСБ, Устремленная в Будущее” [“The FSB, Looking to the Future”], *New Times*, February 19, 2018, https://newtimes.ru/articles/detail/147619.

586 “Опрос показал, хотят ли россияне карьеры разведчика для своих детей” [“Survey Shows Whether Russians Want an Intelligence Officer Career for Their Children”], *RIA Novosti*, November 5, 2019, https://ria.ru/20191105/1560570969.html.

587 “ФСБ, ГРУ, ФСО, СВР… не боги” [“The FSB, GRU, FSO, SVR…Are Not Gods”], Glagolurfo.com, December 16, 2020, http://glagolurfo.com/newsitems/2020/12/16/fsb-gru-fso-svr-ne-bogi/.

588 Rid, *Active Measures*, 431.

589 Corera, *Russians Among Us*, 301-03.

590 Lydia Saad, “Majority of Americans Now Consider Russia a Critical Threat,” Gallup, February 27, 2019, https://news.gallup.com/poll/247100/majority-americans-consider-russia-critical-threat.aspx.

591 Jeffrey M. Jones, “Fewer in U.S. Regard China Favorably or as Leading Economy,” Gallup, March 2, 2020, https://news.gallup.com/poll/287108/fewer-regard-china-favorably-leading-economy.aspx.

592 Christine Huang, “Views of Russia and Putin Remain Negative Across 14 Nations,” Pew Research Center, December 16, 2020, https://www.pewresearch.org/fact-tank/2020/12/16/views-of-russia-and-putin-remain-negative-across-14-nations/.

593 The video can be found at https://www.youtube.com/watch?v=liohDIOc8Fo&feature=youtu.be.

594 “Russia's FSB Disciplines Future Officers Over SUV Parade Stunt,” *Radio Free Europe/Radio Liberty*, July 14, 2016, https://www.rferl.org/a/russia-fsb-future-officers-disciplined-parade-stunt/27858804.html.

595 "Record $185M in Cash Seized From Russian Official in Sting Operation," *Moscow Times*, May 20, 2019, https://www.themoscowtimes.com/2019/05/20/185m-seized-from-ex-fsb-official-in-corruption-scandal-a65658.

596 "Seven FSB Officials Have Been Arrested in a Robbery Case. They May Have Also Stolen Money during Searches of corrupt Officials," *Meduza*, July 5, 2019, https://meduza.io/en/feature/2019/07/05/seven-fsb-officials-have-been-arrested-in-a-robbery-case-they-may-have-also-stolen-money-during-searches-of-corrupt-officials.

597 Robert Grenier, "Spies, Lies and Sneaky Guys: Human INTelligence in the Digital Age," presentation made for the University of Delaware Global Agenda Speaker Series, March 21, 2012, https://www.youtube.com/watch?v=bfIxarRLMDo.

598 Christopher Walker, "What is 'Sharp Power'?," *Journal of Democracy* 29, no. 3 (July 2018): 9-23, https://www.journalofdemocracy.org/articles/what-is-sharp-power/.

INDEX

A

Abel, Rudolf. *See* Fisher, William
Able Archer, Exercise, 176
active measures, 83, 145, 190–197
advanced persistent threat. *See* APT
Agabekov, Georgiy. *See* Arutyunov, Georgiy
agents provocateurs, 24–25
AGI. *See* auxiliary general intelligence ship
al-Assad, Bashar, 96
Aleksandr III, Tsar, 21, 24
Aleksandr II, Tsar, 21
All-Russian Cooperative Society (ARCOS), 33
All-Russian Extraordinary Commission for Combating Counterrevolution and Sabotage (VChK), 12, 22, 29, 37, 153
All-Union Society for Cultural Relations with Foreign Countries (VOKS), 124
Ames, Aldrich, 15, 229
Amtorg Trading Company, 33, 137, 155
Andropov, Yuriy, 44, 44–45, 53, 87, 98, 212, 273
"Anonymous Bulgaria", 196
Anschlag, Andreas and Heidrun, 115, 226, 227
APT (advanced persistent threat), 68, 256–258
  APT28 (aka Fancy Bear), 161
  APT29 (aka Cozy Bear), 161
Araks satellite (also called Arkon-1), 254
ARCOS. *See* All-Russian Cooperative Society
Artamonov, Aleksey (aka Janosh Neumann), 158
Arutyunov, Georgiy (aka Georgiy Agabekov), 25, 31, 32, 211
Aulska chlorine plant, 182
auxiliary general intelligence ship (AGI), 247–249
Avio Spa, 142

B

Badin, Dmitry Sergeyevich, 129
Bakatin, Vadim, 45, 54–55, 60, 61
BALTOPS, 248
Bandera, Stepan, 208
Barmine, Alexander. *See* Graff, Aleksandr
Bashneft, 157
Basmachis, 31
Baykonur launch complex, 252, 259
Bellingcat, 69, 128, 129, 210, 212
Belousova, Alisa (aka Eas7), 163
Berezovsky, Boris, 122, 127, 207
Beriya, Lavrentiy, 38, 39, 43, 53
Berzin, Yan, 48
Beslan, Chechnya, 68, 93, 205
Bezrukov, Andrey (aka Donald Heathfield), 57, 226, 227
Bianchi, Maurizio Paolo, 142
Bittman, Ladislav, 191
Bochkarev, Mikhail, 125
Bombardier (Canadian aircraft manufacturer), 149
Borah, William, 26
Bortnikov, Aleksandr Vasilyevich, 58, 69
Botyan, Aleksey, 187
Boyce, Christopher, 229
Brazhnikov, Aleksandr, 142
Browder, William, 157
Budennovsk, Stavropol Krai, 60
Bundestag, 122, 124, 129, 254
Bureau of Revolutionary Propaganda, 31
Burtsev, Vladimir, 28
Buryakov, Yevgeniy, 15, 147–149, 151, 221, 228
Bush, George, 264
Butina, Mariya, 87, 123, 123–124, 231

C

Carney, Jeffrey, 238
Central Intelligence Agency (CIA), 9, 11, 14, 15, 23, 57, 89, 95, 125, 194, 211, 225, 243, 270
Chapman, Anna, 124, 226
Chayka, Yuriy, 56
Chebrikov, Viktor, 239
Chechnya, 50, 55, 68, 91, 92, 96, 188, 189, 203, 205, 208, 264
chekist, 19, 38, 43, 53–58, 60, 65, 72, 75, 77, 96, 210, 273
Cherepanov, Aleksandr, 89
Cherepanov, Sergey (aka Henry Frith), 226, 227
Cherkalin, Kirill, 158
Chizhov, Vasiliy, 54
Clinton, Hillary, 109, 121, 197, 227, 264
close access technical operations, 110, 121, 235, 245–247, 259
Cohen, Morris and Lona, 223
Colby, Bainbridge, 33
"color revolutions", 54, 57, 189, 264
Committee for State Security. *See* KGB
Committee of Information (KI), 41, 75
communications intelligence (COMINT), 239, 250
Communist International (Comintern), 32–34, 47
computer-based attacks, 159, 180–182
computer-based collection, 117–118, 159, 162, 180, 256–258
Council of People's Commissars, 31, 37, 38, 39
Counterintelligence Directorate (UKR) SMERSH, 40, 67

cover, illegal, 222–227, 234
cover, legal, 139, 217–221
cover, nonofficial (NOC), 221–222
Cozy Bear. *See* APT29
cyber. *See* computer-based attacks or computer-based collection

D

DCLeaks, 196
Deflektor, 237, 247
de las Heras, Afrika, 223
Delisle, Jeffrey, 114, 115, 116, 127
Democratic National Committee, 75, 120, 121, 129, 197, 254
demokratizatsiya, 45
Deryabin, Petr, 51, 97, 154
Director of National Intelligence, 79, 80
disinformation, 26–27, 107, 119, 145, 159, 189, 191–197, 198, 267, 272
diversionary intelligence group (DRG), 179, 183, 188, 198
Dmitrievski, Kristian, 142
double agent, 27–29, 40
Drugov, Fedor, 22
Dulles Plan, 54, 272
Dutch Safety Board, 128, 197
Dzerzhinskiy, Feliks, 33

E

Eas7. *See* Belousova, Alisa
economic counterintelligence, 82, 152
economic intelligence, 63, 82, 144–159
elections targeting, 118–121, 197
electronic intelligence (ELINT), 239, 249–254
Energetic Bear, 161
"ENORMOUS", 174
European Union, 106, 109, 194
Extraordinary Commission for Combating Counterrevolution and Sabotage (ChK), 21

F

Fancy Bear. *See* APT28
Farewell Dossier, 139
Federal Agency for Government Communications and Information (FAPSI), 58, 60, 68, 239
Federal Border Guard Service. *See* FPS
Federal Protective Service. *See* FSO
Federal Security Service. *See* FSB
Federal Tax Police, 75
Fisher, William (aka Rudolf Abel), 223
Fitin, Pavel, 41
Foreign Intelligence Service. *See* SVR
Foreign Policy Concept of the Russian Federation, 96, 104, 177
FPS (Federal Border Guard Service), 58, 65
Frenzel, Alfred, 122
Frith, Henry. *See* Cherepanov, Sergey
Frolov, Dmitry, 158
FSB (Federal Security Service), 12, 58, 60, 65–69, 73, 75, 76, 86, 89, 98, 155–159, 239, 241, 268
  Alfa, 68, 208
  Border Guard Service, 67
  Center 16 (Military Unit 71330), 68, 242
  Center for Information Security (TsIB), 68
  Counterintelligence Service, 66
  Department K, 153, 158
  Department P, 153
  Department T, 153
  Economic Counterintelligence Service, 152

Economic Security Service, 67
Military Counterintelligence Service, 40, 67
Service for the Defense of the Constitutional Order and Fight Against Terrorism, 66, 91
Vympel, 68, 208
FSK (Federal Counterintelligence Service), 58
FSO (Federal Protective Service), 60, 69–71, 73, 100
Fuchs, Klaus, 174

G

Gebrev, Emilian, 210
geospatial intelligence (GEOINT), 254–256
Gidis, Jose Maria, 28
Ginzberg, Samuel (aka Walter Krivitsky), 32, 34, 46, 47, 48, 136, 147, 223
glasnost, 11, 45
Gorbachev, Mikhail, 44–45, 56, 130
Gordievsky, Oleg, 23, 103, 104
Gouzenko, Igor, 170, 174, 232
GPU. *See* State Political Directorate
Graff, Aleksandr (aka Alexander Barmine), 47
Great Purge (Yezhovshchina), 17, 29, 38, 40, 43, 51
Greenglass, David, 174
GRU (Main Intelligence Directorate of the Soviet Armed Forces General Staff), 42, 46–50, 75, 113–117, 136, 138, 165–173, 181, 236, 254
6th Directorate, 236, 239, 253
Spetsnaz, 199
Unit 26165 (85 Special Service Main Center), 197, 253
Unit 29155, 198, 207
Unit 54777 (72nd Special Service Center), 198
Unit 74455 (Main Center for Special Technologies, GTsST), 197
GUGB (Main Directorate for State Security), 38
GU (Main Directorate of the General Staff), 73–75
GUO (Main Administration of Protection), 58, 60
Guriyev, Lidiya and Vladimir (aka Cynthia and Richard Murphy), 57, 109
Gusev, Stanislav, 110, 246

H

Haftar, Khalifa, 201
Hanssen, Robert, 15, 127, 219, 229
Haswani, George, 151
Heathfield, Donald. *See* Bezrukov, Andrey
Helfand, Leon, 35
Hendler, Mikhail (aka Mikhail Stein), 33
Hero of the Russian Federation, 17, 75, 187, 265
Hoover Institution Archives, 11
Howard, Edward Lee, 15, 229
human intelligence (HUMINT), 108–110, 113–117, 122–124, 132, 142, 217–234

I

IG Farbenindustrie, 137
IL-20 SIGINT aircraft, 250, 251
IL-22PP SIGINT/electronic warfare platform, 250
Impuls, 245
InfoRos, 198
Intelligence Department. *See* Razvedupr
International Democracy Foundation, 11

International Department (INO), 30, 34, 61
Islamic State, 151, 196, 200
ITAR-TASS news agency, 148

J

Jeffries, Randy Miles, 15
Jobbik Party, 109
Joint State Political Directorate (OGPU), 25, 26, 30, 32, 38, 147, 203
Joyal, Paul, 207

K

Kalugin, Oleg, 23, 122, 180, 211, 212, 243, 244
Karetnikov, Aleksey, 226, 227
Karpov, Petr Mikhailovich, 26–27, 147, 154
Kaznacheyev, Aleksandr, 196, 229
KGB (Committee for State Security), 12, 13, 22–24, 23, 44–45, 51, 53–61, 54, 73, 87, 89, 106, 138, 139, 179, 190, 210, 212, 229, 236, 239, 241
- 1st Chief Directorate, 61, 75, 136
- 1st Chief Directorate, Department 16, 238
- 3rd Chief Directorate, 25, 30, 67
- 5th Directorate, 25, 29, 54, 58, 67, 98
- 9th Directorate, 69
- 13th Department, 179
- Directorate T, 63, 138

Khangoshvili, Zelimkhan, 69, 202
Khodorkovsky, Mikhail, 156
Khokhlov, Yevgeniy, 43, 223
Khudaverdyan, Tigran, 100
Kiselnikova, Raya, 233
Kochnev, Dmitriy Viktorovich, 70
Kometa, 254
Kondor program, 255
Konoplev, Vladimir, 139
Kopatskiy, Aleksandr, 211
Korobov, Igor Valentinovich, 74
Korshunov, Aleksandr, 15, 142
Kostyukov, Igor Olegovich, 74
Kouzminov, Alexander, 223
Kovacs, Bela, 109
Kovalev, Nikolay, 71
Koval, George, 17
Kozyrev, Andrey, 55
Krivitsky, Walter. *See* Ginzberg, Samuel
Kryuchkov, Vladimir, 45, 61, 104, 130, 176
Kudirka, Simas, 154
Kutepov, Aleksandr, 25, 207
Kutsik, Mikhail, 227

L

Lazaro, Juan. *See* Vasenkov, Mikhail
Lenin, Vladimir, 34, 48
Liana program, 253
Liman, 249
Line EM, 232
Line KR, 63, 232
Line N, 232
Line OT, 233, 245
Line PR, 63
Line SK, 232
Line X, 63, 139, 142
Litvinenko, Aleksandr, 122, 127, 207, 212
Lotos-2, 253
Lourdes, Cuba, 240, 244
Lyalin, Oleg, 179, 182, 219

M

MacKinlay, Andrew, 122
MacMillan, James, 89, 233, 238

Maersk shipping line, 182
Magnitsky, Sergey, 157, 158
Magomedov, Ali, 97
Main Administration of Protection. *See* GUO
Main Directorate of the General Staff. *See* GU
main enemy concept, 35, 42, 54
Main Intelligence Directorate of the Soviet Armed Forces General Staff. *See* GRU
Malaysian Airlines Flight MH17, 127, 195, 197
Malinov, Nikolai, 110
Manhattan Project, 17
Marin, Yuri Michael. *See* Pyatakov, Yuriy
Markov, Georgy, 206
Martin, William, 229
Massing, Hede, 224
MB (Ministry of Security), 58
McCarthy, Joseph, 42
measures of support, 63, 145, 149, 191
MGB. *See* Ministry of State Security
MI5, 103
military intelligence, 27, 46–50, 82, 165–186
Military Topographic Division of the General Staff, 254
Mills, Patricia. *See* Perevezeva, Natalya
Ministry of Foreign Affairs, 41, 57
Ministry of Internal Affairs (MVD), 40, 71, 100
Ministry of Security. *See* MB
Ministry of State Security (MGB), 25, 40, 238
Mitchell, Bernon, 229
Mitrokhin, Vasiliy, 27, 138, 175, 178, 180, 190–191, 243
Möller, Martin, 113
Molotov-Ribbentrop pact, 11, 35, 48
Monarchist Organization of Central Russia (MOTsR), 28
Mondich, Mikhail, 40, 211
Morozova, Anna, 187
Murphy, Cynthia and Richard. *See* Guriyev, Lidiya and Vladimir
MVD. *See* Ministry of Internal Affairs

N

Naryshkin, Sergey Yevgenyevich, 65, 69, 222
National Guard of the Russian Federation (Rosgvardiya), 71–73
National Intelligence Priorities Framework (NIPF), 80
National Security Council, 79
NATO. *See* North Atlantic Treaty Organization
Navalny, Aleksey, 98, 157, 158, 202, 203
Nazi party, 35, 43, 44, 48, 187
Near Abroad, 54, 75, 106
Nemtsov, Boris, 98, 203
Nestorovich, Vladimir, 211
Neumann, Janosh. *See* Artamonov, Aleksey
Nicholson, Harold, 15
Nikolayev, Lev. *See* Orlov, Alexander
Norris, George, 26
North Atlantic Treaty Organization (NATO), 73, 104, 106, 109, 113–117, 127, 128, 139, 176, 185, 194, 207, 248, 249, 264
Norwegian Parliament Building, 125, 246
Nosenko, Yuriy, 89
NotPetya, 181, 182, 188
Nunn May, Alan, 174

O

Obama, Barack, 227, 264
OGPU. *See* Joint State Political Directorate
Okhrana, 11, 19, 21–29
Okno Outer-Space Control System (SKKP), 241
Okolovich, Georgiy, 207
"Olympic Destroyer", 183, 198
Open Skies Treaty, 184, 271
Operation INFEKTION, 192, 196
Operation RYaN (nuclear missile attack), 175
Operation Trest (Trust), 28, 30
Opperput, Eduard. *See* Upeninsh, Aleksandr
Organization for the Prohibition of Chemical Weapons (OPCW), 111, 129, 246
Orlov, Alexander, 9–10, 81–83, 138, 153, 211
Orlov, Vladimir, 26
Ovakimyan, Gaik, 137
Ovchinnikov, Ivan, 240

P

Palaez, Vicky, 57
Patricof, Alan, 227
Patrushev, Nikolai, 156
Pelton, Ronald, 15
Penkovsky, Oleg, 169
People's Commissariat for Internal Affairs (NKVD), 9, 38
People's Commissariat of Foreign Affairs (Narkomindel), 31
perestroika, 11, 45
Perevezeva, Natalya (aka Patricia Mills), 227
persona non grata, 218
Petrova, Yevdokiya (aka Kartseva), 41, 233
Petrov, Vladimir. *See* Shorokhov, Afanasiy
Pitts, Earl, 15
Podobniy, Viktor, 148
Poeteray, Raymond, 115, 227
political intelligence, 63, 81, 103–130
Politkovskaya, Anna, 203
Polyakov, Dmitriy, 169
Popov, Petr, 168
Poretskiy, Ignatiy (aka Ignace Reiss), 32, 47, 137, 146
Poteyev, Aleksandr, 225
Presidential Security Service, 70
Primakov, Yevgeniy, 12, 191
Putin, Vladimir, 21, 44, 46, 53–54, 56, 60–61, 65, 69, 72, 86–88, 91, 97, 98, 106, 122, 130, 131, 143, 155, 156, 195, 200, 205, 225, 263–265
Pyatakov, Yuriy (aka Yury Michael Marin), 211, 247
Pyatnitskiy, Osip, 32

Q

Qadhafi, Moammar, 189, 264

R

Radio-electronic Intelligence, 236
Radio Free Europe, 230
radio-technical intelligence. *See* signals intelligence
Raketa, 245
Rastvorov, Yuriy, 88, 228
razvedka, 46, 187, 198
Razvedupr, 32, 46, 47
Rebet, Lev, 207
Registupr (Registration Department), 46
Reilly, Sydney, 24
Reiss, Ignace. *See* Poretskiy, Ignatiy

Repin, Mikhail, 122, 228
Rezun, Vladimir (aka Viktor Suvorov), 138, 199, 228
RIMPAC, 248
Rose, Fred, 121
Rosenberg, Julius and Ethel, 174
Roskomnadzor, 100
Rosneft, 65, 151, 157
Rostec, 142, 149, 239
Round the World Trading Company, 155
RUNET, 101
Rusnano, 141
Russian Oil Products, 146
Russian Orthodox Church, 221, 229
Russophiles National Movement, 110
Russophobia, 8, 189, 273

S

Sabca, 139
sabotage, 41–45, 179–180, 181
Sabotka, Anton, 15
Salimanov, Georgiy, 211
San Francisco Russian Consulate, 139, 244, 270
Saracoğlu, Sukru, 88
Saudi Red Crescent, 156
SAVAK (Iran), 180
science and technology (S&T) intelligence, 63, 136–144
Sechin, Igor, 151, 157
Semenko, Mikhail, 226, 227
Semyonov, Yulian, 44
Sergun, Igor Dmitriyevich, 74
Šešelis, Romanas, 151
Seventeen Moments of Spring, 44, 54
Shelaputin, Vadim, 25
Shevchenko, Arkadiy, 230, 244
Sheymov, Viktor, 237
Shorokhov, Afanasiy (aka Vladimir Petrov), 89, 219
signals intelligence (SIGINT), 110–111, 139, 197, 236–251
Simm, Herman, 113
Sipelgas, Aleksandr, 223
Skripal, Sergey, 129, 169, 195, 212, 219, 267
SMERSH. *See* Counterintelligence Directorate (UKR)
Smolenkov, Oleg, 212
Snowden, Edward, 127, 268
Society for Social Reform, 156
SODCIT. *See* Strategic Operation for the Destruction of Critically Important Targets
SoftBank, 150
SolarWinds, 161, 163, 258
Sorge, Richard, 43, 223
SORM. *See* System for Operational Investigative Measures
Sovfracht, 150
Spanish Civil War, 9, 48
spearphishing, 90, 128, 181
Special Section (OO), 25, 30, 40
Sporyshev, Igor, 148, 151
Stalin, Iosif, 9, 28, 34, 35, 38, 39, 43, 47–49, 51, 53, 106, 130, 137, 138, 147, 179
Stashynsky, Bogdan, 212
State Duma, 98, 100, 157
State Political Directorate (GPU), 38
State Security Workers Day (Chekists Day), 57
Stein, Mikhail. *See* Hendler, Mikhail
Strategic Defense Initiative (Star Wars), 176
Strategic Operation for the Destruction of Critically Important Targets (SODCIT), 177, 178, 181, 247
Strauss, Robert, 54

Sudmalis, Imant, 187
Sudoplatov, Pavel, 13, 41
Suvorov, Viktor. *See* Rezun, Vladimir
SVR (Foreign Intelligence Service), 12, 61–65, 73, 81, 108, 113–117, 144, 150–151
  Directorate ER, 63
  Directorate KR, 63
  Directorate MS, 63
  Directorate NTR, 63
  Directorate OT, 64
  Directorate PR, 62
  Directorate S, 63
  Zaslon, 64
System for Operational Investigative Measures (SORM), 99, 241

T

Telegram, 100
The Intelligence Officer's Deed, 43
TLSContact, 89
Torshin, Aleksandr, 123, 124
Tretyakov, Sergey, 108, 150, 232
Trilisser, Mikhail, 32
Trotsky, Lev, 31, 47
Trump, Donald, 264
Tsarev, Oleg, 12
Tselina program, 251–254
Tu-142 maritime reconnaissance, 251
Tu-214R SIGINT collection and targeting aircraft, 250
Tukhachevskiy, Mikhail, 40, 48
Tumanov, Oleg, 230
Turla. *See* Venomous Bear

U

Umerenko, Yevgeniy, 142
Unified Space System (EKS Kupol), 255
United Engine Corporation (UEC), 142
United Nations Iran-Iraq Military Observer Group (UNIIMOG), 113
Upeninsh, Aleksandr (aka Eduard Opperput), 28
US-A (Active Guided Satellite), 253
U.S. Department of State, 192, 246
U.S. Peace Corps, 156
US-P (Passive Guided Satellite), 253

V

Vasenkov, Mikhail (aka Juan Lazaro), 57, 226
Vasilyev, Andrey, 158
Vassiliev, Aleksandr, 12
Vavilova, Yelena (aka Tracy Lee Foley), 57, 224, 226, 227
VChK. *See* All-Russian Extraordinary Commission for Combating Counterrevolution and Sabotage
Venomous Bear (aka Turla), 68, 161
Venona program, 16
Vetrov, Vladimir, 139, 219
Viktor Leonov, AGI, 248
VneshEconomBank, 148, 221
Volodarsky, Iosif, 137, 146
Von Karman Institute for Fluid Dynamics, 139
Von Stierlitz, Max Otto, 44
Voodoo Bear, 181
Vorontsov, Sergey, 145
Vostochniy Launch Site, 259
Vyugin, Oleg, 158

W

Wagner Group, 201
Walker, John, 15, 229, 233, 238
Warnig, Matthias, 152

Warsaw Pact, 106, 174, 240, 251, 264
Westinghouse Electric Company, 160
Whelan, Paul, 87
Wikileaks, 196
Workers and Peasants Red Army (RKKA), 30
World Anti-Doping Agency (WADA), 183, 197, 246
World Economic Forum (WEF), 110, 247

Y

Yagoda, Genrikh, 38
Yakovlev, Aleksandr, 11
Yakushev, Aleksandr, 28
Yandex, 100
Yantar (cartographic satellite program), 254–255
Yantar (undersea research ship), 184, 249
Yarovaya Law, 100
"Year of the Spy", 15, 125
Yeltsin, Boris, 54, 56, 58, 263
Yezhov, Nikolay, 38
Yezhovshchina. *See* Great Purge
Yukos, 156
Yurchenko, Vitaliy, 15

Z

Zaitsev, Mikhail, 238
Zatuliveter, Katia, 123, 124, 231
Zenit (counterintelligence intercept program), 245
Zenit (satellite program), 254
Zhiganov, Oleg, 123
Zhigunov, Aleksandr, 88
Zolotov, Viktor Vasilyevich, 71, 72

A COMPREHENSIVE OVERVIEW OF RUSSIAN INTELLIGENCE

Kevin Riehle delivers the definitive guide to Russian intelligence and security—an indispensable resource for sorting through and interpreting the huge amounts of publicly available information about Russian clandestine and covert activities today. The core responsibility of the Russian intelligence services is to preserve the Russian regime and protect it from internal and external threats. This book explains the organization of the services, the missions they undertake, and the human and technical platforms they use. This comprehensive volume:

- Uses a case-based approach to show current missions and functions.
- Avoids the hyperbole often found in media portrayals of Russian intelligence.
- Explains the historical interplay between Russian intelligence and security elements.

Kevin Riehle spent over 30 years in the U.S. Government as a counterintelligence analyst studying foreign intelligence services, finishing his government career as an associate professor of strategic intelligence at NIU. He received a Ph.D. in war studies from King's College London, an MS of strategic intelligence from the Joint Military Intelligence College (an NIU forerunner), and a BA in Russian and political science from Brigham Young University. Today he is an associate professor at the University of Mississippi. Dr. Riehle has written on a variety of intelligence and counterintelligence topics, focusing on the history of Soviet and Eastern Bloc intelligence services. In 2020, he published *Soviet Defectors: Revelations of Renegade Intelligence Officers, 1924-1954*. His articles have appeared in *Intelligence and National Security*, *International Journal of Intelligence and Counter-Intelligence*, *Cold War History*, and *Journal of Intelligence History*, and he has been interviewed by the International Spy Museum for its Spycast podcast series.

ISBN 978-1-932946-10-9
90000>
9 781932 946109