Report

Confronting the Russian Hydra

Continuity and Innovation in the Grey Zone

| Ivan U. Kłyszcz | Marek Kohv |

December 2025

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

Title: Confronting the Russian Hydra: Continuity and Innovation in the Grey Zone
Authors: Kłyszcz, Ivan U; Kohv, Marek
Publication date: December 2025
Category: Report

Cover page photo: A sculpture of Lavrentiy Pavlovich Beria, former chief of secret police under Joseph Stalin, is displayed during an auction preview for "The Cold War Relics Auction - Featuring the KGB Espionage Museum Collection" at Julien's Auctions in Beverly Hills, California, on 8 February 2021. Frederic J. Brown / AFP/ Scanpix

Keywords: active measures, CheKa, Cold War, disinformation, espionage, hybrid warfare, influence operations, intelligence services, strategic culture, Russia

ISSN 2228-0529
ISBN 978-9916-709-57-3 (print)
ISBN 978-9916-709-58-0 (pdf)

63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Contents

Acknowledgements

The authors wish to thank Dr Sanshiro Hosaka for his thoughtful comments and input, as well as the participants from the "Grey Zone Activities in Estonia and Japan: Threats and Responses" webinar, held on 11 December 2024. All statements of fact and judgment are the responsibility of the authors only.

About the Authors

Ivan U. Klyszcz

Dr Ivan U. Klyszcz joined the ICDS as a Research Fellow in September 2022. Previously, he was a full-time doctoral researcher at the University of Tartu, where he obtained his PhD in international relations. Dr Klyszcz's research is centred on issues of international security, namely, great power competition, the grand strategy of major powers, and Russian foreign policy. In recent years, Dr Klyszcz has investigated the drivers, methods, and impact of Moscow's global international relations – particularly with Africa, Latin America, and South Asia – and their implications for European strategy. In addition, he has studied Russian domestic politics, with a focus on centre-region relations, Chechnya and the North Caucasus. Since 2019, he has published over 60 articles, including research reports, peer-reviewed articles, and policy memos, as well as delivered presentations at academic and policy conferences across Europe and North America. Dr Klyszcz has been quoted in international media such as *Al-Jazeera, BBC, France 24*, and *The Economist*. His work has been cited by peer researchers and attracted the interest of diplomats, governments, and major NGOs. Dr Klyszcz is a member of PONARS Eurasia and a frequent contributor to *Riddle Russia*.

Marek Kohv

Marek Kohv joined the ICDS in 2024 as a 20-year security and national defence veteran. His last position in the public sector was Head of Analysis at the Government Office's National Security and Defence Coordination Bureau. Among his other duties, Marek Kohv was in charge of several analytical products aimed at maintaining situational awareness for the Prime Minister and Government ministers. Throughout his career, Marek Kohv has also served in the Defence Forces in various positions, including in the Military Intelligence Centre and Joint Headquarters of the Estonian Defence Forces. He has participated in several foreign operations in Iraq and Afghanistan. Marek Kohv is an alumnus of the United States Army John F. Kennedy Special Warfare Center and School as a Psychological Operations officer. He holds a master's degree in European Union and international law from Tallinn University of Technology.

List of Abbreviations

ARCOS	All-Russian Co-operative Society
BRIC	Brazil Russia India China
CheKa	All-Russian Extraordinary Commission (*Всероссийская чрезвычайная комиссия*, USSR)
DGSE	Directorate-General for External Security (*Direction Générale de la Sécurité Extérieure*, France)
Comintern	Communist International (*Коммунистический Интернационал*)
CPUSA	Communist Paryt of the United States of America
FIMI	foreign information manipulation and interference
FSB	Federal Security Service (*Федеральная служба безопасности*, Russia)
GRU	Main Directorate (*Главное управление*, Russia)
KAPO	Internal Security Service (*Kaitsepolitseiamet*, Estonia)
KGB	Committee for State Security (*Комитет государственной безопасности*)
NKVD	People's Commissariat for Internal Affairs (*Народный комиссариат внутренних дел*)
OGPU	Joint State Political Directorate (*Объединённое государственное политическое управление*)
R&D	research and development
SVR	External Intelligence Service (*Служба внешней разведки Российской Федерации*)

Executive Summary

The leading threat to European security today, Russia's aggressive foreign policy is enacted in part by its intelligence services. The dizzying array of hybrid threats surfacing every month across the continent can obscure the fact that Moscow's agencies behave along well-known tendencies. To highlight the continuity, evolution, and innovation in Russian strategy, this report draws attention to the legacies and enduring trends in order to help better understand the logic behind Russian covert operations and, more importantly, forecast the shape these might take in the future.

Crucially, the Russian services have preserved a Bolshevik paranoid view of international affairs, where the suspicion of conspiracy turns all foreign actors into potential threats. In this institutionalised worldview, their cause is always righteous, entrenching a mindset where no limits as to how to engage a perceived enemy apply. Explored in two different chapters, this report walks the reader through the strategic culture and established doctrine of the Russian services (Chapter 1), with special attention to active measures, disinformation campaigns, and sabotage operations (Chapter 2).

The services push narratives that reflect the features of their strategic culture. Namely, they favour consistent themes that echo their paranoia about international affairs, their sense of moral superiority, and the supposed irrationality and aggressiveness of the west. Many of these elements emulate Soviet-era communist propaganda.

The Russian services draw from a long lineage of aggressive covert operations from the Bolshevik era to the Cold War. Externally, these aimed at narrowing the gap between the Soviet Union and its more technologically advanced rivals. Internally, stories about supposed sabotage, allegedly carried out by foreign operatives, served as both an instrument of propaganda and a justification for repression. The services of today have rediscovered sabotage – now increasingly common on European soil – as a tool in their campaign to dissuade the west from supporting Ukraine.

To confront these rising threats, government and non-government stakeholders must proactively mitigate vulnerabilities across all domains:

- Societal resilience. An informed public, with media literacy skills and access to independent journalism, will be able to resist Russian information operations.

- Cyber and information defence. Strengthen critical targets through preventive measures (e.g., risk-based cybersecurity) and responsive strategic communications.

- Secure critical infrastructure. Energy grids, transport hubs, and especially, undersea cables and pipelines require monitoring, patrolling, and public-private cooperation.

- Economic statecraft. Reduce strategic dependencies to undermine the levers of influence that actors may exploit to amplify the impact of covert operations.

- Alliance coordination. Achieve hybrid deterrence through cross-domain playbooks, shared attribution standards, and graduated response.

- Measuring success. Confronted by hybrid threats, defenders must assess their resilience across sectors. Transparency will, in turn, ensure political will.

"Imagination is its own form of courage"

Frank J. Underwood, a fictional US President
House of Cards by Netflix

Introduction

In Estonia – and Europe more broadly – no other foreign power is seen as more of an imminent threat than the Russian regime of Vladimir Putin. Not only because of Russia's 2022 full-scale war of aggression against Ukraine, but also because of Moscow's constant use of malign covert operations across the European continent.[1] These episodes demonstrate that the Kremlin's belligerence is not restricted to Ukraine. According to the Czech foreign ministry, out of approximately 500 suspicious incidents documented in the European Union (EU) in 2024, 100 could be attributed to Russian covert operations.[2] Worldwide, Russian disinformation has been found attempting to shape the national politics from the US to Estonia.

This is primarily the result of the Kremlin's decision to wage war against Europe, overtly in Ukraine and covertly elsewhere on the continent. Indeed, all the main Russian services have been put under international sanctions for their subversive activities, referred to by the Council of the European Union as "destabilising actions abroad."[3] The Russian intelligence agencies – the civilian Federal Security Service (FSB) and External Intelligence Service (SVR), and the military Main Directorate (better known as the GRU), all commonly referred to as 'the services' – are the main actors behind this hybrid offensive.[4]

In modern-day covert actions, social media and the wider internet multiply the impact of operations, while the goal stays the same: i.e., to strike fear and sow confusion among target populations. This applies to disinformation campaigns but also in some instances of sabotage, where the overt operational goal is to 'send a message' to policymakers and society. There is continuity in the attitudes, methods, and techniques deployed by the Russian and Soviet services alike. These reflect the enduring legacies of the Bolshevik intelligence agencies, especially the often-mythologised CheKa.

Understanding the lineage, mindset, and *modus operandi* of adversarial intelligence services has become a necessity across Europe. The two chapters in this report combine the expert knowledge about the past of the services with their contemporary operations – in that sense, both the new horizons and the enduring legacies. The first chapter, by Ivan U Klyszcz, analyses the features of the 'chekist mindset' and how it influences disinformation. The second chapter, by Marek Kohv, examines the long-standing use of sabotage techniques by the Russian services, from their Bolshevik origins to the present day.

[1] Charlie Edwards, "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure," *IISS*, 19 August 2025.

[2] "Up to 100 'suspicious incidents' in Europe can be attributed to Russia, Czech minister says," *Reuters*, 4 December 2024.

[3] "Russian hybrid threats: EU agrees first listings in response to destabilising activities against the EU, its member states and partners," Council of the European Union, 16 December 2024.

[4] The GRU, however, is Russia's main military intelligence agency, while the FSB and SVR are civilian services. These two former ones are in the lineage of the KGB, which involves a sense of rivalry and distrust towards the GRU. Anecdotally, GRU staff is referred by some former-KGB personnel derisively as "the boots" (*сапоги*).

Chapter 1. The Strategic Culture of the Russian Intelligence Community

Ivan U. Klyszcz

The traditions of chekism must be eradicated, it must cease to exist as an ideology.

Vadim Bakatin, the KGB's last director, 1992

In many parts of the world, a growing sense of international instability has settled, driven by risks such as climate change, economic dislocation, and political polarisation. Among these factors, rivalry between major powers features as a top concern for respondents across the world, while covert operations and foreign subversion make up a significant element of this worry. According to the Munich Security Index 2025, respondents in 11 states worldwide found that – on average – cyberattacks are the fourth most pressing security risk for their country, with disinformation ranking tenth.[5]

In the case of Europe, few other actors compare in belligerence in the information space to the Russian intelligence agencies. In part, this is a reflection of the persistent organisational culture in the Russian services, which predisposes them to take risks, act recklessly and without concern for norms or human lives.[6] The Russian intelligence agencies are often thought of as reproducing the culture of their Bolshevik predecessors, sometimes referred to as the chekist mindset (*чекистское мышление*) or chekism. As historian Calter Walton suggests, during the wars of the Romanov succession:

> [e]vidence of western secret conspiracies left a burning impression in the hallways of the Kremlin that lasted throughout the Soviet era. Its echoes still reverberate there today.[7]

The culture of the CheKa, inherited by the services of today, may, in turn, be referred to as the strategic culture of the Russian intelligence community. This term implies the "cultural assumptions and biases" that policy makers carry with them when analysing strategic issues.[8] What is the strategic culture of the Russian intelligence community? How is it reflected in their *modus operandi*? In this brief chapter, an answer to these questions is outlined by drawing from the specialist literature, documents of the KGB and the modern-day services, and from relevant references to the directors of the Russian services. To explore how the strategic culture of the services shapes their aggressive posture, this chapter presents the case of Russian disinformation as a concrete example.

1.1. The Services

For decades, the Kremlin has sought to cultivate a sense of continuity between the Russian intelligence community and the CheKa – or rather the mythologised version of it. The service had a relatively brief existence (1917–26), but it set out several patterns of behaviour and thought lasting even into the present day.[9] This continuity is in part upheld by the cult of Felix Dzerzhinsky – Vladimir Lenin's loyal intelligence chief – whom the

The Kremlin has sought to cultivate a sense of continuity between the Russian intelligence community and the CheKa

[5] The countries polled were Brazil, Canada, China, France, Germany, India, Italy, Japan, South Africa, the United Kingdom, and the United States, with polls taking place in November 2024. Tobias Bunde, Sophie Eisentraut, and Leonard Schütte, *Munich Security Index 2025* (Munich Security Conference, 2025).

[6] See: Amy Knight, *Putin's Killers: The Kremlin and the Art of Political Assassination* (Biteback Publishing, 2019).

[7] *CheKa* is the Russian acronym for the All-Russian Extraordinary Committee. Calder Walton, *Spies: the epic intelligence war between east and west* (Hachette UK, 2023), 43.

[8] There is a vast academic literature on the concept of strategic culture. Some key references include: Jack L. Snyder, *The Soviet strategic culture: Implications for limited nuclear operations* (1977), and Yitzhak Klein, "A theory of strategic culture," *Comparative strategy* 10, no. 1 (1991): 3–23. This citation is from Alan Bloomfield, "Time to move on: Reconceptualizing the strategic culture debate," *Contemporary security policy* 33, no. 3 (2012): 450.

[9] See: Vadim Birstein, *SMERSH: Stalin's Secret Weapon* (Biteback Publishing, 2013), 16.

Soviets made into an object of adoration, with cities, monuments, and poetry dedicated to him. Despite being the architect of the Bolshevik Red Terror (in which tens of thousands died as part of large-scale repression campaigns), the Soviets memorialised Dzerzhinsky as a compassionate leader, an effective administrator, and a dedicated patriot. Indeed, a phrase that every chekist should have "a cold head, a warm heart and clean hands" *(холодная голова, теплое сердце и чистые руки*), attributed to him, was made into the slogan capturing the chekist ethos idealised by the Soviet regime.[10]

Beyond slogans, however, the Bolshevik and later Soviet services did cultivate something akin to a professional *esprit du corps* in their ranks, one that would ensure their loyalty to Moscow. A confessed loyalty to Marxism-Leninism was central, but this element was not essential, especially as the genuine commitment to communism waned over time, including in the services.[11] Indeed, the Russian intelligence community often refers to their predecessors as acting in the service of 'defending the Motherland' rather than defending socialism.[12]

The professional ethos fostered a sense of superiority and innocence, as well as a shared geopolitical outlook on confrontation between the socialist and capitalist worlds. More so than ideology, this ethos or organisational culture, as historian Emmanuel Droit argues, was among the factors that facilitated the survival of the services across eras.[13] Its flexibility also enabled the survival of the chekist mindset after 1991, as the communist trappings were replaced with a conservative undertone, whereby reflecting the leanings of the Putin era.[14]

Central to this continuity was the lack of accountability for Soviet crimes against humanity

Central to this continuity was the lack of accountability for Soviet crimes against humanity, many perpetrated by Moscow's intelligence agencies. Indeed, elite continuity was a feature of the 1990s, as the Soviet elites – the *nomenklatura* (*номенклатура*) and the party members – maintained their authority across society. According to estimates by Maria Snegovaya and Alexander Lanoszka, members of the old Soviet elite still made up the majority of the Russian elites as of 2020. Consequently, they conclude, this continuity allowed for the survival of belief systems from the Soviet era.[15] For the Russian intelligence services, continuity was just as pronounced, if not more.[16] Therefore, the Soviet era cult of Dzerzhinsky and the chekist mindset were reinvented for the new authoritarian politics of post-Soviet Russia.[17]

The chekist mindset was reinvented for the new authoritarian politics of post-Soviet Russia

Finally, other organisational features, such as the constant competition among the services, can be inferred. Indeed, the overlapping missions of the FSB, GRU, and SVR mean that they are locked into a rivalry over resources

[10] The phrase features prominently in Soviet and Russian secret service manuals. Andreï Kozovoï, *Les Services secrets russes* (Tallandier, 2020), 74.

[11] Andrei Soldatov and Irina Borogan, "Dead Water: How the Russian Security Services' Paranoid Mindset Justifies the War," *Stockholm Centre for Eastern European Studies*, Guest Report 5 (2022): 4.

[12] "Александр Бортников: ФСБ России свободна от политического влияния [Aleksandr Bortnikov: Russia's FSB is free from political influence]," *Rossiyskaya Gazeta*, 19 December 2017.

[13] See: Emmanuel Droit, *Les polices politiques du bloc de l'Est. À la recherche de l'Internationale tchékiste, 1955-1989* [The political polices of the East bloc. The search of the Chekist international, 1955-1989] (Gallimard, 2019).

[14] Julie Fedor, *Russia and the cult of state security: the Chekist tradition, from Lenin to Putin* (Routledge, 2011), 122.

[15] Maria Snegovaya and Alexander Lanoszka, "Reclaiming What Is Ours: Elite Continuity and Revanchism," *European Journal of International Security* (October 2024): 9–13.

[16] See: Sanshiro Hosaka, "Unfinished Business: 1991 as the End of the CPSU but Not of the KGB," *Demokratizatsiya: The Journal of Post-Soviet Democratization* 30, no. 4 (2022): 441–452.

[17] See: Fedor, *Russia and the cult of state security*, 121–122.

and the Kremlin's attention.[18] In turn, this rivalry results in their entrepreneurial attitude to covert operations. Moreover, diverse backgrounds of these agencies contribute to their unique cultures, with the GRU being more reliant on high-stakes operations (reflecting its military character) and the SVR being more risk-averse.[19] Here, however, the focus is on what brings the services together, and the shared chekist mindset that is found throughout the community.

1.2. The Chekist Mindset

The chekist mindset – the strategic culture of the services – can be narrowed down to four key elements: a superiority complex, an insistence on their own innocence, paranoia, and, especially in recent years, extremism. As the following shows, these distinct characteristics overlap with and reinforce one another. Some reflect broader trends in Russian political culture, as well as commonplace tropes from the Soviet era. Yet, when put together, they may be considered features forming the worldview common in Russian intelligence community.

1.2.1. Superiority

In 2000, then-FSB director Nikolay Patrushev referred to his personnel as a "modern neo-nobility" (*современное неодворянство*).[20] This expression did not take root, but officers often portray themselves as exemplars of patriotism and loyalty to public service, as well as having elite capabilities and skills. To put Patrushev's statement into perspective, the British MI6 recruitment website refers to "talented people," while the French Directorate-General for External Security (DGSE) emphasises its openness to candidates' diverse backgrounds.[21]

The analogy to the supposed nobility – in terms of being both service-minded and elite – of today's Russian intelligence community traces its origins to the Bolsheviks. In the Leninist worldview, the Communist Party was the vanguard of the proletariat, meant to change the ruling class from the bourgeoisie to the working class, and thus establish the dictatorship of the proletariat. Within this framework, the CheKa and its successors were the vanguard of the vanguard, and a key instrument to thwart the enemies of the revolution.[22] As Lenin stated in a speech delivered in 1918, "[t]he important thing for us is that the Cheka is directly exercising the dictatorship of the proletariat, and in that respect its services are invaluable."[23] In short, for the communists, the secret services are a cornerstone of real, existing socialism, so they exalted their role in – what we may call – national security and society more broadly.[24]

This sense of exaltation has continued since the fall of the USSR. For example, one local FSB chief described the members of the services as having a sense of being "the chosen ones" (*избранные*): "I do not know by whom exactly – God, the Party, or the people – but this chosenness (*избранность*) is something we treasure."[25] The reverse side of being the chosen ones is loyalty to the intelligence community and to Putin, as the top leadership sets the tone and the agenda.[26]

Across these eras, the sense of superiority has led the services both to a sense of paternalistic protection of the Russian population and a contemptuous distance

[18] As of 2025, the full-scale Russian invasion of Ukraine may have attenuated this rivalry somewhat. Namely, the presidential administration may have emerged as a coordinator and leader of the Russian intelligence community. This means that the Russian services are now governed by coordination rather than by competition. The Doppelgänger disinformation campaign reflects, to an extent, this coordination. See: Martin Laine and Anastasiia Morozova, "Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections," *VSquare*, 16 September 2024.

[19] Mark Galeotti, *Russian political war: Moving beyond the hybrid* (Routledge, 2019), 89.

[20] Fedor, *Russia and the cult of state security*, 135.

[21] "Explore careers at SIS," Secret Intelligence Service MI6, accessed on 19 March 2025; "Nos modes de recrutement [Our recruitment modes]," DGSE, accessed on 19 March 2025.

[22] James Sherr, *Hard diplomacy and soft coercion: Russia's influence abroad* (Brookings Institution Press, 2013), 26–32.

[23] Vladimir Lenin, "For The All-Russia Extraordinary Commission Staff," *Izvestia* 214, 10 November 1918.

[24] See: Yaacov Falkov, "Intelligence-Exalting Strategic Cultures: A Case Study of the Russian Approach," *Intelligence and National Security* 37, no. 1 (2021): 90–108.

[25] Leonid Mlechin, "Из чекистов в неодворяне [From Chekists to neo-nobility]," *Kommersant*, 4 December 2017.

[26] Galeotti, *Russian political war*, 62–66.

from them. Here, references abound to the services compassionately defending the Russian population against various threats, including even "spiritual" ones.[27] According to FSB Director Alexander Bortnikov, national security also involves preventing internal conflicts and the destruction of the state, like in the "collapse of the Russian empire" and the "breakdown of the Soviet era."[28]

1.2.2. Innocence

The principal goal of the early CheKa and its successors was to act as a political police that also engaged in counterintelligence.[29] So, the history of all the intelligence agencies under Moscow's authority has been one of repression, mass surveillance, and active participation in crimes against humanity. This is known internationally but also in Russian society, where, each year since 1991, on 30 October, the Remembrance Day for the Victims of Political Repression is observed (by some).[30]

The history of all the intelligence agencies under Moscow's authority has been one of repression, mass surveillance, and active participation in crimes against humanity

Forced to deal with this reputation, the Russian intelligence community insists on its innocence as well as on the righteousness of its cause and that of its predecessors. For example, a revealing case was the attempted rehabilitation of Lavrenti Beria – Stalin's spy master and architect of the Great Terror – in the 2000s. A 2008 book connected to the Russian intelligence community portrayed Beria as an "effective manager," justifying his crimes against humanity as "necessary."[31] Similar portrayals, emphasising competence and selflessness, were made of Dzerzhinsky and Andropov, who were again turned into cult-like figures under Yeltsin and Putin, in both cases cast as well-meaning and even "saintly."[32] Sincerity and honesty were valued virtues among the chekists throughout the Cold War, but also today.[33]

Behind this narrative is a sense of self-preservation and innocence. For example, since the Khruschev era, the Russian services have insisted that they, too, were victims of the Stalin purges, thus minimising their role as perpetrators. For example, Bortnikov stated in 2017 that "the 'purges' began with the [security] organs," stressing their supposed victimhood.[34] To reiterate, the Soviet slogan describing the CheKa insisted on the officers' "clean hands," often described as part of the service's "humanism."[35] Similar allusions are made today: Bortnikov has claimed that the FSB is "free from political influence," unlike the Communist KGB, which, in turn, should lead people to trust the service.[36]

The Russian services have insisted that they, too, were victims of the Stalin purges, thus minimising their role as perpetrators

Combining the presumptuous sense of superiority and innocence is the trend, prevalent within the community, to resent those periods when authorities constrained their power. For example, First Secretary Nikita Khruschev's assertion of party control after Stalin's Great Terror is remembered "as a time of humiliation and catastrophe for the security apparatus."[37] The attempts in the early 1990s to dismantle the powerful KGB are bitterly remembered and dramatised as "attempts […] to destroy the very system of the country's state security."[38]

[27] Fedor, *Russia and the cult of state security*, 160–181.
[28] "Aleksandr Bortnikov."
[29] Walton, *Spies*, 39.
[30] "Say their names. Why remembering the victims of Soviet-era repression is more about Russia's future than its past," *Novaya Gazeta Europe*, 3 November 2024.
[31] Birstein, *SMERSH*, 39.
[32] Fedor, *Russia and the cult of state security*, 24, 125, 143.
[33] Droit, *Les polices politiques du bloc de l'Est*, 31.
[34] "Aleksandr Bortnikov."
[35] In the Soviet era, allusions to humanism were of "Socialist" humanism, as opposed to "bourgeois" humanism. Fedor, *Russia and the cult of state security*, 16–18.
[36] "Aleksandr Bortnikov."
[37] Fedor, *Russia and the cult of state security*, 30.
[38] Quoted in Fedor, *Russia and the cult of state security*, 125.

1.2.3. Paranoia

The services' over-estimation of threats – both in their prevalence and imminence – is often treated as the distinctive feature of the chekist mindset.[39] This paranoid thinking is directed at foreign threats but has a dual dimension: foreign intervention and the 'fifth column'. In a 2017 interview, Bortnikov stated that unnamed foreign powers have always wished for "the destruction of Russia" (*разрушение Россию*), and today, foreign intelligence agencies are "attempting to penetrate every sphere of our state."[40] Like with the sense of innocence, paranoia also reinforces the services' case for their role and importance in society. Indeed, pointing to continuous external threats has served the services to avoid accountability and downsizing.[41]

Pointing to continuous external threats has served the services to avoid accountability and downsizing

This sense of paranoia is also rooted in mistrust towards society, ingrained in the services' mission of political policing. The Soviet system hinged on the notion of a socialist elite – the party and the *nomenklatura* – meant to drive society towards communism under the dictatorship of the proletariat. This model lacked democratic legitimacy, so the Soviet leaders, too, constantly lacked trust towards their own population. Indeed, the Soviet leadership often accused the country's population of harbouring 'counter-revolutionary forces'. This lack of trust was amplified into paranoia by the intelligence services, whose primary task was (and is) political policing. The wars of the Romanov succession left an imprint here, as well. As historian Calder Walton writes, "[t]he Bolsheviks faced armed western intervention to depose them. Many other enemies were phantoms."[42] Paranoid conspiracy theories are popular among the Russian services of today.[43]

Today, the theory of 'counter-revolution' conspiracies has remained the Kremlin's preferred framework to understand political changes abroad, especially in the proximity to Russia. As Kent DeBenedictis argues, in the Putin era, the thinking habits of the socialist-era theory of counter-revolution became prevalent again among Russia's leadership; this time, under the label of 'colour revolutions'.

The theory of 'counter-revolution' conspiracies has remained the Kremlin's preferred framework to understand political changes abroad – this time, under the label of 'colour revolutions'

According to this theory, revolutions have been taking place across the countries of the Middle East and North Africa because of plots, masterminded in the west and activated by NGOs and via other channels.[44] This threat assessment is shared by the Russian secret services. For example, as SVR Director Sergey Naryshkin commented in 2024 about the Georgian political crisis, "[t]he west never lets go of its victim so easily. Today, Tbilisi, faces yet another attempt at a colour revolution, that is, an attempt at a coup d'état."[45] Here, the conspiracy theory of NATO and the west 'encircling Russia' illustrates a common theme that also shapes the services' paranoid threat perception.

1.2.4. Extremism

Combining these three preceding elements – superiority, innocence, and paranoia – is the rising extremist views in the Russian services. This extremism is underwritten by a narrative of political messianism, a long-standing current in Russian political thought.[46] Today, Russian messianism envisions the restoration of the country's greatness and role as a major power, including control over several

[39] Soldatov and Borogan, "Dead Water."
[40] "Aleksandr Bortnikov."
[41] Droit, *Les polices politiques du bloc de l'Est,* 39.
[42] Walton, *Spies*, 40.
[43] Soldatov and Borogan, "Dead Water," 6–7.
[44] Kent DeBenedictis, *Russian 'hybrid warfare' and the annexation of Crimea: the modern application of Soviet political warfare* (Bloomsbury Publishing, 2022), 17–19, 27, 31–41.
[45] "Нарышкин прокомментировал ситуацию в Грузии,[Naryshkin commented on the situation in Georgia]" *RIA Novosti*, 26 November 2024.
[46] Peter Duncan, *Russian messianism: third Rome, revolution, communism and after* (Routledge, 2002).

independent countries, such as Ukraine. In turn, this restoration is seen in global terms as the harbinger of a 'multipolar' world order, a supposedly more 'just' order waiting to emerge.[47]

This zero-sum narrative can be interpreted as extremism. According to J. M. Berger, extremist groups are defined by the belief that their survival can only be guaranteed by the harm caused to an out-group construed as threatening. In this view, the in-group is defined as inherently legitimate and righteous, while the target out-group is fundamentally illegitimate and actively menacing.[48] The origin of the chekist extremism also goes back to the historical CheKa. The organisation was conceived to carry out the revolutionary violence meant to tear down the old order and create a new, socialist society.[49]

A similar messianic narrative forms the political mainstream of today's Russia, and the country's intelligence community is a key proponent of this outlook on global affairs. Indeed, the 'noble' service is framed in terms of "[restoring] Russia's dignity on the world stage."[50] In turn, this narrative serves to further legitimise the intelligence agencies' authority over society, as the services see themselves as ordained by destiny to secure Russia.[51] For the chekists of the past and of today, the result is a blurring of peace and wartime, justifying constant offensive measures against their perceived adversaries by making special use of covert operations. Not only is Russia in a constant state of perceived siege, but any advantage for Russia can only be discerned in terms of how disadvantageous it is to the US, the 'main adversary'. For example, when commenting on the controversial electoral victory of the Russia-leaning Georgian Dream party, Naryshkin said it was a "defeat" (*провал*) for Washington.[52]

For the chekists of the past and of today, the result is a blurring of peace and wartime, justifying constant offensive measures against their perceived adversaries

1.3. Disinformation: A Natural Choice

Russian disinformation has been closely scrutinised in recent years. It is identified as a key instrument of statecraft for the Kremlin, one that enables it to meddle in the politics of foreign countries across the world. Due to its clandestine nature, we do not have a complete outline of the resources and capacity deployed by the Kremlin for its information warfare. Some known figures point to its large scale. One 2025 estimate by the Ukrainian Center for Counteracting Disinformation suggests that the Russian Ministry of Defence spends $100 mn annually on disinformation campaigns targeting Ukraine.[53] According to the European External Action Service, in 2024, Ukraine remained the top target of Russian information manipulation and interference operations in Europe (257 recorded incidents), followed by France (152).[54]

The scope of the disinformation campaigns is global, exerting a persistent pressure on targets through opportunistic action. For example, in 2024, Russian state-controlled media spread disinformation narratives targeting Japan's engagements with Central Asian states, specifically meant to thwart the Central Asia + Japan Summit.[55] That narrative repeated many hallmarks of Russian disinformation, such as the allegation that US allies were nothing but Washington's puppets rather than independent states, a smear often levelled at Estonia and all NATO members, as well as Japan.

[47] Alicja Curanović, *The sense of mission in Russian foreign policy: destined for greatness!* (Routledge, 2021).

[48] J. M. Berger, *Extremism* (MIT Press, 2018), 39, 65.

[49] Droit, *Les polices politiques du bloc de l'Est*, 33.

[50] Fedor, *Russia and the cult of state security*, 137.

[51] Fedor, *Russia and the cult of state security*, 142.

[52] "Нарышкин заявил о провалах США на постсоветском пространстве [Naryshkin spoke about the failures of the US in the post-Soviet space]," *Mezhdunarodnaya Zhizn*, 10 December 2024.

[53] Olena Mukhina, "Russia spends over $ 1 billion annually on disinformation campaigns," *Euromaidan Press*, 21 February 2025.

[54] "3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the architecture of FIMI operations," EEAS, 19 March 2025, 9.

[55] "DISINFO: The West is trying to undermine the friendship between Central Asia and Russia," *EUvsDisinformation*, 8 August 2024.

1.3.1. Planning and Implementation

Conceiving and planting disinformation narratives is the work of several departments found in each of Russia's major intelligence agencies. The ingrained strategic culture of the services inclines them to (over)estimate the value of disinformation, FIMI, and information warfare more broadly. Indeed, disinformation could be considered one of the main operational techniques of the Russian intelligence community, and among the ones with the longest lineage.[56] Disinformation was part of Russia's intelligence agencies since the Tsarist era, when St Petersburg ran operations from a station in Paris. On 11 January 1923, the CheKa established its disinformation department, with the mission to "deter military intervention by the western powers" through "disinformation for western military intelligence services."[57] Exploiting an unforeseen opportunity, their first target was the White Russian exile community, executed by an agent who was then based in the then-recently independent (1918) Estonia, previously under the Romanov rule.[58]

The ingrained strategic culture of the services inclines them to (over)estimate the value of disinformation, FIMI, and information warfare

Later in the Cold War, the KGB's First Department (dealing with external intelligence and operations) established a department dedicated exclusively to disinformation, Directorate D (for *дезинформация)*. In the transition from communism, the First Department was spun off the KGB into a new civilian intelligence body, the SVR. So, the accumulated expertise on operational techniques mostly survived into the post-Soviet era. Several units inside the GRU run disinformation campaigns, with its Fifth Department in charge of information warfare operations, and the FSB's Eighth and Sixteenth centres engaged in these activities, too.[59]

Today, Russian intelligence is known to refer to its disinformation operations as part of 'measures of support' (*мероприятия содействия*), a broad label applied to covert operations.[60] While the techniques and environment of these measures might be different, they resemble the Cold War-era KGB 'active measures' (*активные мероприятия*). Those were conceived by the KGB "to exert influence on the adversary" in the context of "[a] secret form of political struggle."[61] The covert and clandestine activities of today are called 'support' measures because they are designed as acts that add to Russia's overall foreign policy. In other words, disinformation and other covert actions are not conceived to be implemented in a vacuum.

The covert and clandestine activities of today are called 'support' measures because they are designed as acts that add to Russia's overall foreign policy

Many of the departments within the Russian services that engage in disinformation are also actively carrying out propaganda campaigns, cyberattacks, and other measures.[62]

Indeed, the disinformation campaigns are deployed after meticulous preparation that can last for months. Part of the preparations sometimes includes establishing key performance indicators, such as documented organic online interactions with the disinformation narrative. According to some accounts, the disinformation campaigns are not expected to pay off instantaneously, with the first results sometimes planned on short-, medium-, and long-term timelines. The campaigns are often intended to be traceless, so preparations draw from intelligence gathering and a deep knowledge of the target's

[56] Kevin P. Riehle, *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present*. (National Intelligence Press, 2022), 24–27.

[57] Quoted in Thomas Rid, *Active measures: The secret history of disinformation and political warfare* (Profile Books, 2020), 25.

[58] Rid, *Active measures,* 20–25.

[59] Galeotti, *Russian political war*, 25.

[60] Riehle, *Russian Intelligence*, 191.

[61] Quoted in Ivo Juurvee, *The Resurrection of 'active Measures': Intelligence Services as a Part of Russia's Influencing Toolbox* (Hybrid CoE, 2018), 3.

[62] Galeotti, *Russian political war*, 35.

context (though often shaped by biases).[63] Hacking campaigns and the cultivation of contacts in media organisations are also part of the preparations.[64] The channels of dissemination vary: planted news stories in foreign media, narratives spread by state-controlled outlets such as *RT* and *Sputnik* (as well as regionally-focused *TV BRICS* and *African Initiative*), independent organisations publish–ing 'leaks' but without means for verification, and unauthentic social media activities (bots).[65] Front organisations run covertly by Russian intelligence also disseminate narratives and cooperate with agents of influence. Combined, these channels form an entire ecosystem that captures audiences and feeds them disinformation.

1.3.2. Narratives

While it is impossible to accurately predict future Russian disinformation narratives, an awareness of the strategic culture of the Russian intelligence agencies can help generate some expectations. Indeed, the narratives are not haphazard. There are documented cases where disinformation narratives are conceived or at least explicitly approved by the director of the service.[66] Top intelligence officers are part of the chekist strategic community, thus generally exhibiting the chekist mindset, as the comments by Bortnikov, Naryshkin, and Patrushev suggest.

Russian disinformation narratives often repeat several consistent themes

Russian disinformation narratives often repeat several consistent themes. These are identified by some analysts and scholars and include: 'Russia's leading role in the Second World War'; 'Russia as a victim'; 'the west as the source of global instability'; 'NATO as a threat'; and 'the EU on the verge of collapse'.[67] While the exact contours change and adapt, these themes reflect several features of the chekist mindset.

The recurrent narratives about the Second World War (or rather the 'Great Patriotic War' of 1941–45, as it is referred to in Russia) capture all four features of the chekist mindset. Indeed, they connect the services of today to the mythologised finest hour of Soviet intelligence in the fight against Nazi Germany. The Second World War underpins a narrative about the righteousness of the Soviet and Russian causes. Moreover, the paranoia is reflected in recurrent disinformation narratives about how any authority or individual who criticises the Russian government has a direct connection with the historical nazis or is a fascist sympathiser.[68] Finally, the extremism is reflected in how this narrative portrays Russia's adversaries – as fundamentally evil and single-mindedly oriented at destroying Russia.

Russia's self-portrayal as a victim in international affairs fully reflects the chekist mindset, especially its paranoia about foreign powers conspiring to target the country. Relatedly, portraying NATO, the US, and the west more broadly as aggressive is a common theme in Russian disinformation campaigns. So, for example, a 2020 narrative about the Defender Europe 20, a NATO exercise of that year, construed the manoeuvres as a provocation.[69] Another simultaneous narrative responded to the EU accusation of Russia for spreading COVID-19 disinformation by alleging that the Europeans did not present any facts to back up their claims. Not only was this a false narrative, but it also alleged that the accusations were driven by a hatred of Russia.[70] Both of these narratives were spread by FSB-run front organisations.[71]

[63] Christo Grozev, Roman Dobrokhotov, Michael Weiss, "'Morality and ethics should play no part': Leaks reveal how Russia's foreign intelligence agency runs disinformation campaigns in the West," *The Insider*, 4 July 2024.

[64] Hacking and information operations sometimes go together in what are sometimes called "hack-and-leak" attacks. See: Rid, *Active measures*, 358.

[65] "3rd EEAS Report on Foreign Information Manipulation and Interference Threats," 14–19.

[66] Examples of this go back to the services' first chief, Felix Dzerzhinsky. Rid, *Active measures*, 23.

[67] Riehle, *Russian intelligence*, 194.

[68] Olga Bertelsen, "A Blind Spit of Active Measures," in *Russian Active Measures: Yesterday, Today, Tomorrow*. (Ibidem-Verlag, 2021), 18.

[69] "DISINFO: Military exercise Defender Europe 2020 is an act of war against Russia," *EUvsDisinformation*, 4 February 2020.

[70] "DISINFO: EU cites zero facts about Russia's alleged disinformation on coronavirus," *EUvsDisinformation*, 28 April 2020.

[71] Andreas Rossbach, "Meet the Kremlin's keyboard warrior in Crimea," *Coda Story*, 29 May 2018.

This characterisation of the west is consistent with the services' paranoid threat assessment, including of 'colour revolutions' and of the 'encirclement of Russia'. Examples of this narrative include the long-standing narrative of so-called 'Russophobia', a notion cultivated by the Kremlin and the intelligence agencies. The goal of this disinformation narrative is to construe the foreign policies of independent countries (especially the Baltic states and Ukraine, but also US allies across the world) as being driven by irrational hatred towards Russia rather than by legitimate security concerns over Moscow's aggressiveness.[72]

The goal is to construe the foreign policies of independent countries as being driven by irrational hatred towards Russia rather than by legitimate security concerns

Indeed, the sense of superiority of the services is connected to their sense of being the 'chosen ones' to stand up for Russia against this alleged hatred. Victimhood can also imply innocence, as the attackers are portrayed as acting unprovoked or in pursuit of selfish goals. Portraying Russia as a victim presents the in-group side of the extremist narrative, namely, of being attacked by the malicious out-group.

Finally, the narrative about the EU's alleged collapse is tied to a broader narrative about the supposed decadence of the west. This is a long-standing feature of Moscow's propaganda and disinformation, going back to the Soviet and Romanov periods. The core idea of this narrative in today's formulation is that the west's democratic, liberal, and capitalist governance has transformed European society into an inauthentic self. So, disinformation narratives in this vein include a 2020 message that EU citizens could not buy food due to dysfunctions in the economy and society. This specific narrative was disseminated by *NewsFront*, one of the FSB-controlled front organisations mentioned above.[73]

These narratives reflect both the chekist mindset and several aspects of Russian political culture more broadly. Russia – having none of the features it attributes to 'the decadent west' (Russia being 'a sovereign democracy') – retains the supposedly authentic character of Europe: i.e., Christian and true to tradition. For the Russian intelligence services, this narrative implies the need for 'spiritual security', a paternalistic impulse to protect Russian society against 'decadent' western cultural influence. In concrete terms, spiritual security is construed as a mandate for engaging in broad censorship of society and persecuting religious and minority groups.[74] As explained earlier, the services' sense of superiority involves a paternalistic mission to protect, grounded in a holistic threat assessment that reflects, once again, the services' paranoia. This spiritual dimension to the services' work has driven them to cooperate with the Moscow Patriarchate of the Russian Orthodox Church, known to be close to the Kremlin.[75]

Chapter 2. Russia's Hybrid Warfare

Marek Kohv

This chapter traces the lineage of Russian hybrid warfare from its Soviet roots to contemporary practice. It argues that a recurring mix of regime insecurity, ideological ambition, and pragmatic opportunism had produced a two-track pattern already in the interwar era, well before the Cold War broke out: i.e., outward-facing sabotage and inward-facing campaigns against fabricated enemies. During the subsequent decades, those habits hardened into an institutional playbook of covert confrontation. Today, the same logic underpins a persistent 'hybrid cold war' waged below the threshold of open armed conflict. The chapter closes with forward-looking implications and a layered framework for prevention, resilience, and countermeasures.

[72] Nikita Aronov, "'Comrade Putin, you're a great scientist.' How pro-Kremlin scholars study "Russophobia" and justify war," *The Insider*, 27 March 2023.

[73] "DISINFO: The Europeans can't even buy food for the first time in 75 years, but the EU prefers to remain silent," *EUvsDisinformation*, 11 April 2020.

[74] Fedor, *Russia and the cult of state security*, 178–179.

[75] Fedor, *Russia and the cult of state security,* 169.

2.1. Historical Roots

2.1.1. Patterns

The Soviet state emerged from revolution with a maximalist ideology and a persistent sense of encirclement. Soviet strategic thought, therefore, combined a commitment to world revolution with a historically conditioned insecurity about Russia's exposed borders. The result was a durable logic of 'defensive expansionism', in which pre-emption and forward pressure were framed as necessary for regime survival. Outwardly, clandestine action – sabotage, subversion, and technology acquisition – was used to narrow industrial and military gaps with rivals. Inwardly, the legal-political category of 'wrecking' (*вредительство*) supplied scapegoats for plan shortfalls, manufacturing conspiracies that disciplined society and consolidated authority. Together, these external and internal repertoires normalised coercive practices as routine instruments of governance and state competition, and covert action as routine statecraft rather than an exceptional expedient.[76] This dual structure also codified 'threat inflation' within official discourse: economic shortfalls and policy reversals were attributed to hostile interference rather than planning deficiencies, thereby legitimising extraordinary mobilisation.[77]

External and internal repertoires normalised coercive practices as routine instruments of governance and state competition

In interwar Soviet strategic culture, three features stand out. First, grounded in Leninist doctrine, Bolshevik elites construed the international arena as intrinsically antagonistic, making clandestine instruments an integral extension of ideology and party strategy. Second, structural economic backwardness created strong incentives to acquire technology through espionage while deflecting accountability for domestic missteps via anti-wrecking campaigns. Third, a preference for centralised control rewarded institutions that combined foreign intelligence gathering with domestic coercion, thereby eroding the boundary between external security and internal governance.

2.1.2. Institutions and Tradecraft

Interwar sabotage operations had a functional division of labour. The Red Army's Intelligence Directorate (GRU) focused on foreign military-technical espionage, clandestine procurement, and associated logistics; the state security organs (the Joint State Political Directorate, OGPU, later the People's Commissariat for Internal Affairs, NKVD) fused domestic repression with outward-facing active operations – including assassinations, penetrations, and disruption; finally, the Communist International (Comintern) mobilised front organisations, provided guidance to foreign parties, and delivered covert support to revolutionary movements.[78] This twin-track approach – overt diplomacy paired with covert ideological penetration – rested on plausible deniability. In fact, bureaucratic rivalry between the GRU and the state security organs typically generated redundancy rather than restraint, creating parallel channels for clandestine action.

Tradecraft in this period displayed resourcefulness under constraint. Soviet services favoured nonofficial cover (for instance, as journalists or trade representatives), cooperative societies, and commercial fronts. They relied on 'cut-outs' embedded in labour unions and émigré associations, practised document forgery, and propagated rumours, all of which would later be codified as active measures.[79] Courier networks linked party cells to *rezidentura* (*резидентура*)

[76] Parliament, House of Commons, *Russia No. 2 (1927). Documents illustrating the Hostile Activities of the Soviet Government and Third International against Great Britain* (His Majesty's Stationery Office, 1927); Michigan State University, "The Shakhty Trial," in *Seventeen Moments in Soviet History* (Michigan State University, 1928).

[77] James Harris, "Historian James Harris Says Russian Archives Show We've Misunderstood Stalin," *History News Network*, 26 July 2016.

[78] "History of the Main Intelligence Administration (GRU)," Global Security, last modified on 15 June 1996; "Third International," Encyclopaedia Britannica, last updated on 21 August 2025.

[79] In intelligence and espionage tradecraft, a 'cut-out' is an intermediary used to pass information or instructions between agents in a way that conceals the direct link between them. The cut-out only knows enough to perform the transfer but is not privy to the full identity, mission, or network of those involved, which preserves operational security.

in European capitals, and training regimes prioritised political reliability as much as technical skill.[80] The Comintern provided a logistics and recruitment base globally, while diplomatic missions offered shelter, immunity against prosecution, and communications.

2.1.3. Sabotage and Subversion

Before 1939, industrial and military espionage was a primary task: Soviet collectors targeted aviation, munitions, and heavy industrial know-how to accelerate the USSR's forced-march industrialisation and build a modern army. The aim was, therefore, not merely growth but war preparation.[81] Political influence operations and disinformation complemented theft: Comintern and security services backed 'national liberation' movements, ran front groups, and sought to discredit adversary elites.

Several high-profile cases across the west help illustrate the evolution of the Soviet approach and focus through the interwar period:

Political influence operations and disinformation complemented industrial and military espionage

- **The United Kingdom**: Cambridge recruitment and the All-Russian Co-operative Society (ARCOS) raid. From the early 1930s, Soviet services cultivated the Cambridge milieu that would later become the Cambridge Five.[82] Earlier, in May 1927, British police searched the ARCOS's London premises, exposing Soviet *rezidentura* tradecraft and triggering a break in diplomatic relations.83 The raid revealed signal plans and a safe-house ecosystem tied to trade representation, validating concerns about the overlap of commerce and clandestinity.

- **The Baltic region:** The 1924 communist coup attempt in Estonia. On 1 December 1924, an armed attempt to seize Tallinn's key nodes – planned in concert with Comintern-linked networks – although defeated within hours, demonstrated Moscow's readiness to employ covert force in neighbouring states.[84] Its quick collapse underscored the limits of revolutionary timing when social support is thin, yet it also signalled to regional governments that subversion could be coordinated across borders.

The 1929 coup attempt in Estonia underscored the limits of revolutionary timing when social support is thin, yet it also signalled that subversion could be coordinated across borders

- **Western Europe:** Assassinations and kidnappings of émigré leaders. Soviet executive action targeted anti-Soviet émigrés on western soil, including the kidnapping of 'White' General Evgenii Miller in Paris (1937) and the assassination of Ignace Reiss, one of the heads of Soviet military intelligence in western and central Europe, in Switzerland (1937).[85] Indeed, such 'special tasks' pursued several goals:

[80] A Soviet intelligence station abroad, known as *rezidentura,* is a local operational unit based in a foreign country. It was typically housed in an embassy, consulate, trade mission, or front organisation, and directed by a resident (*резидент*), a senior Soviet intelligence officer in that location. *Rezidentura* coordinated recruitment, managed agents, organised courier networks, and reported intelligence back to Moscow. Holger Weiss, *A Global Radical Waterfront: The International Propaganda Committee of Transport Workers and the International of Seamen and Harbour Workers, 1921–1937* (Leiden; Boston: Brill, 7 June 2021); Central Intelligence Agency, *Transmittal of Document Relative to the Macedonian Question in Yugoslavia*, Information Report (Central Intelligence Agency,17 February 1950).

[81] Judy Welfelt, "From the Editor," *Fairmount Folio: Journal of History* 13 (19 April 2016).

[82] Mark Dunton, "Confessions from the Cambridge Five: a file release from MI5," *The National Archives GOV. UK*, 14 January 2025.

[83] University of Warwick, *The ARCOS Raid and the Break in Anglo-Soviet Relations, 1927* (Modern Records Centre, University of Warwick, 2011).

[84] "History: The 1924 December Coup Attempt in Estonia," *ERR News*, 30 November 2024.

[85] Stephen M. Arness, "Paper Mills and Fabrication," *Studies in Intelligence* 2 (Central Intelligence Agency, 1958); Federation of American Scientists, National Counterintelligence Center, "Chapter 4: Counterintelligence Between the Wars," in *American Revolution to World War* (National Counterintelligence Center, 1996).

to neutralise organisers, sow fear in émigré circles, and demonstrate a willingness to violate host countries' sovereignty while denying responsibility.

- **The United States:** Network building among officials (the Ware Group). In Washington, DC, Soviet sympathisers clustered in the so-called Ware Group, a clandestine Communist Party USA (CPUSA) cell organised c. 1933 inside President Franklin D. Roosevelt's Great Depression-era New Deal agencies; it doubled as a recruitment pool for Soviet intelligence and a channel for espionage, later documented by investigations and memoirs.[86] Notably, the episode illustrates early, opportunistic cultivation of access within open bureaucracies long before Cold War bipolarity crystallised.

Covert violence had been practised earlier, too. The St Nedelya Cathedral bombing in Sofia in 1925 – carried out by the Military Organisation of the Bulgarian Communist Party with alleged external guidance and support – remains a stark interwar example of terrorist sabotage.[87]

2.1.4. The Internal Dimension

Domestically, sabotage was juridically codified as wrecking under the Soviet criminal code (for more, see the sections above). Its elastic definition penalised acts ranging from wilful disruption to negligence or careless execution of duties, thus enabling the attribution of economic failure to enemies rather than policy errors. Early show trials, such as the 1928 Shakhty case, inaugurated 'wreckers' as a class, thereby paving the way for the Great Terror's social cleansing under a rhetoric of anti-sabotage.[88] The distinction between criminality and political subversion had been eroded, and the burden of proof became secondary to the disciplining utility of the charges themselves. The practice inculcated a culture of denunciation and risk-aversion, however, with second-order effects on industrial performance and military innovation.

The elastic definition of wrecking enabled the attribution of economic failure to enemies rather than policy errors

By the late 1930s, the Soviet state had normalised clandestine external disruption and internalised sabotage as political instruments. This architecture foreshadowed the globalised practices of the Cold War.

2.2. The Cold War Blueprint

2.2.1. Active Measures

Soviet doctrine combined ostensibly defensive political narratives with offensive operational concepts. The interwar 'deep battle' tradition (i.e., disruption of mobilisation and command by attacking the system as a whole rather than isolated units) matured into plans to disrupt the enemy's rear throughout the theatre.

In parallel, the KGB (together with the GRU) used to run what came to be defined as active measures: clandestine political warfare encompassing disinformation, forgeries, front organisations, and support to proxies. The value of active measures lies, in particular, in their deniability and the difficulty of verifying provenance.[89] This makes them a force multiplier: cheap to stage, costly for democracies to counter, and effective at corroding trust.

The subsequent toolkit thus combined 'rumour operations' (e.g., fabricated letters and pamphlets), covert media placement, front conferences, support to pacifist movements, and forgeries intended to inflame social cleavages. From a theoretical standpoint,

[86] Whittaker Chambers, "Testimony before the House Committee on Un-American Activities, August 3, 1948," Famous Trials Project, UMKC School of Law, published online in 2003; Allen Weinstein, "IV The Ware Group and the New Deal," in *Perjury: The Hiss-Chambers Case* (Maryland State Archives Document, October 1995).

[87] Veneta Pavlova, "Ninety Years Since the Bomb Attack on St. Nedelya Church," *Radio Bulgaria*, 16 April 2015.

[88] Frank B. Baird Jr and Richard E. Pipes, "Industrialization, 1929–34," Encyclopaedia Britannica, last updated on 26 October 2025.

[89] Vasiliy Mitrokhin (ed), *KGB Lexicon: The Soviet Intelligence Officer's Handbook* (London: Frank Cass, 2002); Jolanta Darczewska and Piotr Żochowski, *Active Measures: Russia's Key Export* (Warsaw: Centre for Eastern Studies, June 2017).

training manuals for Soviet intelligence officers emphasised shaping the target nation's information environment rather than merely collecting secrets. Organisationally, the KGB's Service A units specialised in disinformation, while *rezidentura* stationed abroad cultivated journalists and intermediaries. The point of this refined doctrine was not only to mislead but to exhaust – to impose investigative and political opportunity costs on the adversary.

Building on this foundation, the KGB further consolidated sabotage planning in its Thirteenth Department and exported it to Warsaw Pact allies. In April 1963, Czechoslovakia created the Special Purpose Service (*Služba zvláštního určení*) to plan "diversion, sabotage, marauding and other operations," with objectives to demoralise opponents, downgrade capabilities, and undermine the North Atlantic Alliance's cohesion. The Soviet doctrine also prioritised target countries (e.g., Belgium for NATO HQ; France and Germany for their weight in Allied decision making) and suggested striking US assets indirectly via third countries.[90]

2.2.2. Caches and Targets

A distinctive feature of Cold War planning was the prepositioning of arms and explosive caches across NATO countries for wartime sabotage. Discoveries documented booby-trapped *Molniya* (lightning) devices (a Cold War-era Soviet intelligence cache designed to store clandestine equipment, such as radios, codes, and weapons, or money for use by agents or sleeper networks in the west), hidden caches scattered in western Europe and elsewhere.[91] Strategic targets included ports, rail nodes, power systems, dams, and pipelines. Of such, Canada-focused Operation "Cedar" and a plan targeting the New York port envisaged destroying refineries and oil and gas pipelines to paralyse logistics during the initial period in a potential conflict.[92] Target selection mirrored deep-battle logic, too.

Assassination capabilities were institutionalised in the KGB's executive-action units (later the Fifth Department). The cyanide-spray gun murders of Ukrainian émigré resistance leaders Lev Rebet (1957) and Stepan Bandera (1959) by Bohdan Stashynsky – recounted in court files and academic literature – illustrate both the tradecraft and political intent.[93] Such actions, while rare, had an outsized psychological impact, as émigré circles in western Europe were targeted to breed fear and discourage outspoken anti-Soviet activism. To potential defectors and dissidents inside the Soviet bloc, these assassinations sent a chilling signal that leaving or opposing the regime could carry lethal consequences, even outside Soviet borders. Subliminal message was also directed at western governments and security services, who were reminded of Soviet reach and ruthlessness.

Complementing North American concepts, Soviet-bloc target typologies captured in 1960s planning guides emphasised: (1) energy systems – power plants, refineries, and pipelines (e.g., the Le Havre–Paris pipeline); (2) communications and transport – railways, bridges, tunnels, highways, and major ports (notably, Rotterdam and Antwerp); (3) military special operations hubs (e.g., the US 10th Special Forces Group at Bad Tölz and France's 11th Parachute Brigade in Corsica); and (4) the so-called psychological diversion centres (e.g., the Radio Free Europe office in Munich). These kinetic options were to be paired with active-measures campaigns to magnify social and political effects.[94]

2.2.3. Espionage and Strategic Purpose

Industrial and military espionage remained central, from penetration of the Manhattan Project (by Soviet agent Klaus Fuchs) to acquire atomic weapons secrets to sustained theft from aerospace and defence contractors during the 1970s–80s, compressing

[90] Daniela Richterova, "The Long Shadow of Soviet Sabotage Doctrine?," *War on the Rocks*, 19 August 2024.

[91] Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield* (2001).

[92] Heiki Jakson et al., *Energy in Irregular Warfare* (Vilnius: NATO Energy Security Centre of Excellence, 30 May 2017).

[93] Serhii Plokhii, "The Man with the Poison Gun: Q&A," Harvard Ukrainian Research Institute, 7 February 2017; "Espionage: A Poor Devil," *TIME,* 26 October 1962.

[94] Richterova, "The Long Shadow."

techno-logical cycles and sustaining strategic parity.[95] The objective was, again, to shorten the learning curve and economise scarce R&D resources, a logic repeated today in cyber-enabled theft. Collection priorities tracked weapon system roadmaps: guidance systems, materials, computing, and cryptology.[96]

Sabotage served four interlocking aims: (1) deterrence and disruption – threatening rapid paralysis of logistics and governance to dissuade or blunt a first strike by NATO; (2) political corrosion – weakening Alliance cohesion through deception and agitation; (3) capability compression – narrowing technology gaps via theft; and (4) psychological leverage – sowing uncertainty to magnify limited actions.[97] These aims rested on the conviction that the opening weeks of war would be decisive and that pre-war shaping could predetermine outcomes.

2.2.4. Escalation Ladder and Agent Ecosystem

Declassified Czechoslovak files preserve a granular escalation schema transmitted by Soviet handlers. In peacetime, planners favoured accident-like disruptions (signal failures, unexplained fires, 'random' contamination, etc.) designed to avoid attribution. In the case of crisis or escalation, larger, unmistakably deliberate attacks would be mounted. Should a war break out, pre-planned, system-level sabotage would accom-pany conventional offensives.[98]

This doctrine specified a pyramid of culprits. At the top sat legal-cover officers in embassies trained to run sabotage missions; they managed 'illegals' who surveyed targets, refined plans, and handled explosives.[99] Beneath them were support agents (in charge of safe houses and logistics), access agents (insiders such as engineers or operators), and 'agents-executioners' or 'agents-saboteurs', recruited and activated by radio, coded mail, couriers, or in person. Destructive means could be Bloc-manufactured as well as improvised in theatre.[100]

By the 1980s, sabotage and active measures had been routinised as instruments of Soviet statecraft, ready for activation in crisis and war.

By the 1980s, sabotage and active measures had been routinised as instruments of Soviet statecraft, ready for activation in crisis and war

2.3. Russia's Hybrid Cold War

2.3.1. Continuity and Innovation

Post-Soviet Russia adapted Soviet toolkits to a networked world, where contemporary hybrid warfare integrates military and non-military levers across the grey zone – below Article 5 threshold. The holistic, opportunistic, persistent nature of this approach and its exploitation of open societies has been extensively studied, but is worth em-phasising.[101] Central to it is the so-called Gerasimov doctrine. Not merely a formal doctrine, however, General Valery Gerasimov's (currently, Chief of the General Staff of the Russian Armed Forces) 2013 observations are better read as a statement that non-military

Post-Soviet Russia adapted Soviet toolkits to a networked world

[95] "Klaus Fuchs," MI5 – The Security Service, last updated in 2025; "The Neighborhood Spy: Zacharski-Bell Espionage Case," Federal Bureau of Investigation (FBI), 3 June 2019.

[96] US Congress, Office of Technology Assessment, *Technology and Soviet Energy Availability* (Washington, DC: U.S. Government Printing Office, June 1979).

[97] Nicholas J. Cull et al., *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It – An Analytic History, with Lessons for the Present* (Final Report) (London: LSE Consulting, October 2017).

[98] Richterova, "The Long Shadow."

[99] In intelligence 'jargon', 'illegals' are clandestine intelligence officers who reside under false, non-diplomatic identities in a foreign country.

[100] Richterova, "The Long Shadow."

[101] Christopher S. Chivvis, *Understanding Russian "Hybrid Warfare" and What Can Be Done About It*, Testimony presented before the US House Armed Services Committee (RAND Corporation, 22 March 2017); Arsalan Bilal, "Russia's Hybrid War Against the West," *NATO Review*, 26 April 2024.

means can exceed the power of force when synchronised – a point often misinterpreted in western debate.[102]

From Soviet to modern Russia, three continuities stand out. First, information confrontation remains central: it relies on shaping narratives to fracture consensus, delegitimise institutions, and erode risk tolerance. Second, economisation of force guides the choice of tools – cyber operations, financial covert actions, and proxies achieve outsized effect without large deployments. Third, plausible deniability preserves strategic ambiguity, complicating retaliation and facilitating escalation management.

A key dimension of continuity from the Cold War to today lies in the institutions that carry forward the legacy of active measures

A key dimension of continuity from the Cold War to today lies in the institutions that carry forward the legacy of active measures. Modern Russian hybrid operations are executed by a constellation of intelligence agencies, each with distinct but overlapping mandates.

The GRU, Russia's military intelligence service, remains the most visible actor in sabotage and cyber-enabled disruption. Its operatives have been linked to infrastructure attacks, clandestine operations in Europe, and the use of deniable proxies. The FSB, formally responsible for internal security, has extended its reach outward: running cyber units, leveraging kompromat, and conducting political influence operations that blur the domestic–foreign divide. The SVR, Russia's foreign intelligence service, continues to cultivate human sources abroad, infiltrate political and civic networks, and sustain front organisations and disinformation channels.

Together, these services form a hybrid ecosystem that blends sabotage, espionage, disinformation, and cyber operations. Their activities highlight both innovation and continuity. Whilst the delivery systems have shifted from forged pamphlets to troll farms and malware, the strategic logic – deniability, disruption, and psychological pressure – remains the same.

A hybrid ecosystem blends sabotage, espionage, disinformation, and cyber operations

2.3.2. Information and Influence Operations

On the information battlefield, Russia's state media (*RT, Sputnik*) and proxy content farms seed and amplify polarising narratives. Influence campaigns combine forgeries, fronts, bots, trolls, and covert funding. For instance, US indictments and interagency operations mapped and documented the Internet Research Agency's activities undertaken during the presidential campaign in 2016;[103] more recently, in 2024, the Departments of Justice and Treasury disrupted Doppelganger/Good Old USA operations, seizing domains and sanctioning actors linked to the Kremlin.[104] The preferred Russian tactics, revealed by those investigations, centre around laundering narratives through sympathetic outlets, cultivating useful experts, and micro-targeting communities where social cleavages can be widened. Additional contemporary manifestations point at what analysts term 'strategic vandalism', illustrated by the widely reported 'coffin affair' in Paris staged to embarrass and intimidate a key Ukraine supporter.[105] Moreover, recruitment and tasking for agents-saboteurs has migrated to online spaces – trends that mirror Cold War logic while updating the means of access and cover.[106]

[102] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, 6 July 2014.

[103] "Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations," Press Release, US Department of the Treasury, 4 September 2024.

[104] "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere," US Department of Justice, Office of Public Affairs, 4 September 2024.

[105] See: Florian Reynaud, Damien Leloup, and Antoine Albertini, "Coffins at the Eiffel Tower: Suspicions point to another case of Russian interference," *LeMonde*, 3 June 2024.

[106] Richterova, "The Long Shadow."

2.3.3. Cyber Operations and Energy Coercion

Public attributions and indictments tie GRU units to destructive and espionage-grade cyber intrusions (e.g., NotPetya attack), with charging documents detailing their tradecraft.[107] For instance, the UK and its international partners have repeatedly called out GRU operations, such as those against Georgia in 2019–20.[108] In this realm, too, Russians have blurred the lines between espionage, disruption, and coercion while directly threatening the provision of healthcare, logistics, and energy services. Indeed, for this type of malign actions, the functional goal is to impose friction at decisive moments – elections, mobilisations, crises – while maintaining ambiguity about intent.

The functional goal is to impose friction at decisive moments – elections, mobilisations, crises – while maintaining ambiguity about intent

Energy leverage – above all, natural gas supplies – has long been a political instrument in Moscow's toolkit. Following the 2022 full-scale invasion of Ukraine, Russia's gas pipeline traffic to the EU was sharply curtailed or cut off on multiple routes, triggering an energy crisis – a historic market shock and no-less historic policy response (i.e., the REPowerEU plan to reduce dependence on fossil fuels and accelerate green transition, diversification of suppliers, demand reduction, etc.). The European Commission and the International Energy Agency characterise such Russian behaviour as the weaponisation of gas.[109] The episodes of energy coercion illustrate how physical networks and market psychology can be exploited to pressure democracies without crossing a kinetic threshold.

2.3.4. Proxies and Deniable Force

Careful to stay below the threshold of open interstate war, Russia has perfected the utilisation of private military companies and unattributed forces (the so-called "little green men," *зелёные человечки*, infamous for their role in the annexation of Crimea in 2014). Alongside suspected operations against infrastructure and undersea assets, proxies are essential as they allow imposing costs while maintaining ambiguity, which fits the logic of plausible deniability that is central to hybrid conflict.[110] Additionally, the use of proxies externalises risk, creates bargaining chips, and complicates legal attribution.

Acts of vandalism at sensitive historical sites have become a prominent feature in Russia-linked hybrid activities, especially when aimed at polarising local communities. In Lithuania, prosecutors claimed that three GRU-tasked individuals defaced a monument to Adolfas Ramanauskas-Vanagas, a partisan leader, in Merkinė in January 2024. The suspects trio acted as an organised group and was promised a payment; one suspect partly confessed.[111] Estonia has likewise documented cases of vandalism and intimidation: the Internal Security Service (KAPO) concluded that Russian services were behind several attacks, including the smashing of the window of the interior minister's car, among others.[112] Courts in 2025 also found that GRU-linked operatives ordered acts of arson and vandalism against venues connected to the Ukrainian community to sow fear.[113] Together, these episodes exemplify low-cost, deniable property damage primarily used to seed narratives of instability and ethnic grievance.

[107] School of International and Public Affairs, "NotPetya: A Columbia University Case Study," *SIPA*-21-022.1 (Columbia University, 2021).

[108] "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and International Cyber Attacks," US Department of Justice, Office of Public Affairs, 19 October 2020; "UK Condemns Russia's GRU over Georgia Cyber Attacks," GOV.UK, 4 October 2019; "NCSC Supports Sandworm Advisory," National Cyber Security Centre, 9 October 2020; "GRU Hackers: Destructive Malware and International Cyber Attacks," Federal Bureau of Investigation Wanted List, last updated in 2020.

[109] "EU Action to Address Energy Crisis," European Commission, last updated in 2024.

[110] Bilal, "Russia's Hybrid War Against the West."

[111] "Investigators: Russian GRU Behind Vandalising Lithuanian Partisan Leader's Monument," *LRT News*, 14 May 2024.

[112] "ISS: Russian Special Services Behind Attack on Estonian Minister's Car," *ERR*, 21 October 2024.

[113] "Russia-Estonia Sabotage Arson Ukraine," *Associated Press* (*AP News*), 4 July 2025.

In another high-profile case, in July 2024, western intelligence warned their German counterparts that Russia was planning to assassinate Armin Papperger, the CEO of Rheinmetall, a key munitions supplier to Ukraine; consequently, his personal security had to be raised to the highest level. NATO later confirmed that the plot formed part of a wider Russian sabotage campaign targeting Europe's defence base. The Kremlin routinely denied its involvement.[114]

Authorities across the EU have linked a wave of arson attacks to Russian services, which tend to recruit criminal proxies for the job. In Warsaw, the Marywilska 44 shopping centre caught fire in May 2024 – an instance that was later officially attributed to Russian secret services after a year-long investigation that resulted in arrests.[115] Polish law enforcers charged and detained dozens of members of a broader sabotage network, who were accused of receiving instructions from Russian handlers.[116] These incidents fit a pattern of low-tech operations designed to stress supply chains and stoke public anxiety.[117]

European railway infrastructure has, again, become a recurring target, primarily due to its logistical function in transporting critical freight and military aid to Ukraine. In October 2022, simultaneous cuts to digital radio communication signal cables halted all railway traffic in the north of Germany, which the prosecutors then qualified as deliberate sabotage.[118] In 2024, the Czech transport minister accused Russia of a "thousand" attempts to interfere with European rail signalling and ticketing systems – part of a broader destabilisation effort.[119] Analysts from the Center for Strategic and International Studies, among others, have been tracking multiple rail incidents in Poland as well as the Nordic states.[120] The pattern, developed for such operations, mixes physical tampering, radio interference, and cyber probing to generate outsized disruption.

Suspicious episodes have been many, and they appear to be rather diverse. In July 2024, a parcel ignited at a DHL warehouse near Birmingham (UK). British counter-terror police investigated potential Russian involvement and arrested a suspect under the National Security Act, citing possible coordination with similar cases across Europe. Indeed, a few days earlier, a similar incendiary parcel ignited at DHL's hub at Leipzig/Halle; German media and prosecutors treated it as part of a cross-border plot to test air-freight channels. Western officials later revealed at a briefing that the devices were intended to be placed on cargo planes *en route* to North America.[121]

Poland has emerged as ground zero for much of Russia's recent sabotage push, reflecting its significant role in logistics for military aid to Ukraine. Local authorities have detained dozens of suspects (Polish, Ukrainian, Belarusian, and other nationals) who were accused of arson, reconnaissance, and attempted attacks on behalf of Russian services. Investigators have detailed the recruitment of low-level criminals online, coordinated by handlers in Russia and Belarus. In particular, the Marywilska fire and other arson attacks, as well as rail interference and plots against US and NATO-linked facilities, are cited in indictments. Legal proceedings are in progress, and in some cases, courts have already begun issuing multi-year sentences. In sum, those episodes constitute elements of a hybrid war meant to raise costs for aiding Ukraine.

2.3.6. Inherent Vulnerabilities

Hybrid campaigns exploit institutional openness, free media, decentralised infrastructure, and electoral cycles – the core pillars of a functioning democratic system. They aim to

[114] "Germany Says It Won't Be Cowed by Russia After Reported Plot to Kill Rheinmetall CEO," *Reuters,* 12 July 2024.

[115] "Poland-Russia Sabotage Ukraine War," *AP News*, 29 July 2025.

[116] "Poland-Russia-Ukraine Sabotage Court Prison," *AP News*, 21 February 2025.

[117] Seth G. Jones, "Russia's Shadow War Against the West," *Center for Strategic and International Studies*, 18 March 2025.

[118] "Rail Northern Germany Standstill Due to Technical Issue," *Reuters,* 8 October 2022.

[119] Carl Deconinck, "Russia Trying to Sabotage European Railways, Says Czech Transport Minister," *Brussels Signal*, 5 April 2024.

[120] Seth G. Jones, *Russia's Shadow War against the West* (CSIS, March 2025).

[121] Jamie Grierson, "Romanian Man Arrested After DHL Warehouse Fire Caused by Suspected Russian Device," *The Guardian*, 9 April 2025; Warren P. Strobel and Daniel Michaels, "Russia Plotted to Attack U.S. Planes With Incendiary Devices," *Wall Street Journal*, 8 April 2025.

stretch response capacity across legal, diplomatic, cyber, and informational lanes, turning speed and transparency into vulnerabilities. The most effective defences – resilience, redundancy, and public awareness – require advance investment and coordination, which is politically hard to sustain in peacetime. The result is a persistent action–reaction lag that favours the initiator.

The most effective defences require advance investment and coordination, which is politically hard to sustain in peacetime

Democracies depend on open information flows and trust in institutions. Adversaries exploit this by flooding the media and social platforms with disinformation, as well as by using bots, trolls, fake news, and selective leaks. The speed and low cost of such online manipulation allow dis- and misinformation to spread before fact-checks or rebuttals can catch up, resulting in the erosion of public trust in media and institutions.[122] In fact, the 24/7 news cycle and demand for rapid reporting can amplify false or misleading claims when outlets rush to cover sensational content without full verification. That gives hybrid actors an opportunity to pre-frame narratives, set agendas, or shift public perceptions.[123]

It is precisely because the democratic model of governance allows and accommodates dissent and contestation that hybrid campaigns can be embedded within civil society, media outlets, political parties, or protest movements

In addition to open institutions, democracies often have open, pluralistic societies, characterised by diversity in ethnicity, religion, and political ideology. These, too, can become fault lines, be abused and manipulated by provoking social identity divisions, stoking grievance, and amplifying 'us vs them' narratives. Hybrid threat actors can further exploit them to undermine social cohesion, reduce trust across communities, and complicate consensus. It is precisely because the democratic model of governance allows and accommodates dissent and contestation that hybrid campaigns can be embedded within civil society, media outlets, political parties, or protest movements – all legitimate arenas – making it hard for authorities to distinguish hostile influence from domestic political expression.[124]

Authoritarian or highly centralised systems impose fewer legal, institutional, or moral constraints on surveillance, censorship, covert action, or retaliation. Democracies, in contrast, must balance responses with civil liberties, legal norms, media freedom, and political pluralism, which slows decision-making and limits certain aggressive countermeasures. Democracies often lack centralised control over both information and information infrastructure: media are independent; tech platforms are private-sector actors; civil society and free press enjoy autonomy. Hybrid adversaries thus focus on targeting weak regulatory regimes, engaging in lobbying campaigns, or using third-party platforms and proxies.[125]

Elections, in particular, create predictable windows of vulnerability. Campaign seasons, debates, and media coverage offer hybrid actors rich opportunities: to influence public opinion, smear opponents, inject divisive narratives, and hack or leak materials. Democratic governments, meanwhile, must adhere to the standards of transparency and fairness, thereby limiting

[122] Herb Lin, *Protecting Democracy in an Era of Cyber Information War* (Hoover Institution, 2018); Francesc Badia i Dalmases, "How Democracies Can Overcome Challenges of Hybrid Warfare and Disinformation," *Barcelona Centre for International Affairs* (*CIDOB*), September 2022.

[123] Gregory F. Treverton, *Addressing Hybrid Threats* (Helsinki: European Centre of Excellence for Countering Hybrid Threats, July 2020).

[124] Elsa Hedling, *Social Identities and Democratic Vulnerabilities: Learning from Examples of Targeted Disinformation. Hybrid CoE Paper 24* (Helsinki: European Centre of Excellence for Countering Hybrid Threats, April 2025).

[125] Amanda Paul, "Hybrid Storm Rising: Russia and China's Axis Against Democracy," *European Policy Centre*, 2 May 2025.

suppressive or intrusive responses.[126] Moreover, democratic institutions, such as parliaments, courts, civil oversight bodies, and regulatory agencies, have built-in deliberative and rule-bound procedures that ensure legitimacy but also slow and diffuse responses to fast-moving hybrid threats.

Due to this inherent openness of democratic societies, foreign actors often have multiple points of access – through diplomatic missions, cultural or trade organisations, diaspora networks, NGOs, media outlets, etc. – as well as a legitimate cover to conduct influence operations. Indeed, hybrid campaigns rely on proxies and ambiguity, with operations carried out by non-state actors and intermediaries or via deniable channels. This ambiguity, in turn, complicates attribution and thus response, legal or otherwise. Constrained by (international) law and norms, democracies find it difficult to moderate or restrict influence operations without appearing repressive, particularly when evidence is murky.[127]

2.4. What to Expect

Asymmetry endures. Low-cost, deniable instruments – cyber intrusions, influence operations, and covert financial activity – will remain attractive to malign actors, especially against stronger adversaries and coalitions, as they offer strategic effect without inviting symmetrical retaliation. Their utility lies in imposing cumulative friction at scale while staying below formal thresholds of armed conflict.

Critical infrastructure is a priority target. Interwar attention to dams and rail hubs foreshadows the focus on grid control systems, ports, pipelines, and subsea cables. Moreover, high interdependence within these networks and systems creates cascading risks, whereby limited actions generate disproportionate economic and political effects.

Information is weaponised. The old logic of active measures has migrated to modern platforms that enable micro-targeting, rapid replication, and algorithmic amplification, while hack-and-leak campaigns blend espionage with psychological impact, shaping decision cycles as much as public opinion.

Deniability is strategic. Ambiguity complicates attribution, slows collective decision-making, and muddies the red lines. Actors willing to exploit legal and informational grey zones can achieve coercive leverage while managing escalation risks.

Proxies proliferate. Front organisations, private military companies, criminal intermediaries, and contracted cyber operators distribute operational risk and distance the state from culpability. This modularity shortens mobilisation timelines and enables simultaneous campaigns across multiple domains.

Escalation management shifts to law and finance. Much of the contestation unfolds outside kinetic channels; therefore, credible deterrence will increasingly depend on coordinated sanctions, export controls, asset freezes, and law-enforcement action. Although these tools raise costs and constrain capacity, they also limit the chances of military spillover.

Hybrid warfare combines continuity with innovation

In summary, hybrid warfare combines continuity with innovation. Seeing the historical patterns – from interwar sabotage and Cold War active measures to today's digital campaigns – allows us to identify both stakes and remedies. Liberal democracies must become harder targets without sacrificing their integral attributes – openness, rule of law, free markets, technological edge, and robust civic capacity – but rather by leveraging those in order to deny the benefits of subversion while managing escalation risks.

[126] Eric Rosenbach and Katherine Mansted, *Can Democracy Survive in the Information Age?* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, October 2018).

[127] Beniamino Irdi, "Hybrid Threats and Modern Political Warfare: The Architecture of Cross-Domain Conflict," *Jamestown Foundation*, 2 May 2025.

Conclusion and Recommendations

As Mark Galeotti writes, "[i]n the west, we have historically failed to understand [Russia's intelligence agencies]."[128] This report proposes to bring together our knowledge of the services – including their institutional history, *modus operandi,* and strategic culture – to anticipate their future behaviour. As the chapter by Ivan U. Klyszcz elaborates, four key features have remained consistent across the Russian intelligence community and throughout decades: i.e., superiority, innocence, paranoia, and extremism. It illustrates how the chekist mindset continues to shape the approach to information warfare. In the next chapter,

The chekist mindset continues to shape the approach to information warfare

Marek Kohv explains the value of sabotage – a component of the services' toolkit meant to maximise effects and subvert foreign societies. This, too, reflects the historical experiences of the Bolsheviks who conceived of the international arena as a zone of confrontation and antagonism.

Hybrid and sabotage operations thrive because they exploit and capitalise on ambiguity, surprise, and the seams between civilian and military domains. These very characteristics that make such campaigns difficult to attribute and counter also mean that no single instrument of power – diplomatic, military, or legal

Only by closing vulnerabilities in advance and coordinating across sectors can democracies reduce the initiative that hybrid actors enjoy

– can provide adequate defence on its own. Preventing and mitigating hybrid threats, therefore, requires a whole-of-society approach: strengthening societal resilience, hardening infrastructure, and building agile communication channels. The recommendations that follow are grounded in this logic: only by closing vulnerabilities in advance and coordinating across sectors can democracies reduce the initiative that hybrid actors enjoy.

[128] Galeotti, *Russian political war*, 87.

Societal Resilience

Resilience begins with informed, cohesive publics. Media literacy, independent journalism, and transparent governance shrink the attack surface for disinformation. The Baltic record – distributed strategic-communications capacity and whole-of-society exercises – offers practical precedent. Learning from it, governments should establish minimum standards for: (1) a standing myth-busting unit able to act within hours; (2) a civic curriculum on information hygiene for school-level and adult education; (3) robust firewalls for public-service media; and (4) structured partnerships with platforms to slow coordinated inauthentic behaviour, consistent with the rule of law.

Cyber and Information Defence

Critical infrastructure should be hardened through risk-based cyber-security, red-teaming, and cross-border incident response. Rapid strategic-communications cells can pre-empt and expose influence operations – an approach increasingly used by western services, including proactive declassification. NATO's StratCom Centre of Excellence and the EU–NATO Hybrid Centre of Excellence provide a framework for doctrine development, train-ing, and best practices. Practical measures should include segmented network archi-tectures, assumed breach drills, cyber ranges for operators, and common taxonomies for whole-of-government reporting. In the information space, messenger credibility is decisive: health authorities, defence professionals, and community leaders should be equipped with evidence released in a timely, transparent manner.

Critical Infrastructure

An essential layer of prevention involves securing critical infrastructure against physical sabotage. Energy grids, transport hubs, and especially undersea cables and pipelines represent attractive targets: they are difficult to monitor continuously, expensive to repair, and vital for both civilian life and military command. Recent incidents (including the sabotage of the Nord Stream pipelines in

2022 and multiple cases of unexplained damage to undersea cables around the Baltic Sea and North Atlantic) demonstrate both the feasibility of such operations and their destabilising potential.

Hardening measures can envisage enhanced seabed monitoring with autonomous systems; joint naval patrols in critical maritime zones; stronger cooperation with private telecommunications and energy operators; and building redundancy so that single points of failure cannot paralyse entire sectors. Embedding these precautions into a hybrid-threat counterstrategy ensures that adversaries cannot leverage infrastructure vulnerability to achieve outsized political or psychological gains.

Economic Statecraft

States should reduce strategic dependencies (especially in energy), diversify suppliers, increase financial transparency and oversight to disrupt illicit flows, and calibrate sanctions to degrade hybrid capabilities while minimising spillovers. Post-2022 EU actions demonstrate the scale and speed required to blunt coercion. Sanctions and export controls should be tied to clear behavioural triggers (e.g., infrastructure sabotage, election interference) and paired with investment screening, anti-money-laundering enforcement, and task forces that map beneficiary-ownership networks.

Alliance Coordination and Deterrence

Hybrid deterrence requires cross-domain playbooks, shared attribution standards, and graduated response options spanning law enforcement, financial tools, and cyber counter-operations. Regular EU–NATO exercises on grey-zone scenarios, clear public signalling, and legal practices that allow for applying international law to hybrid activities can close perceived sanctuaries. A credible response menu ranges from joint public attribution and synchronised sanctions to covert disruption of active targeting infrastructure – under thresholds communicated in advance.

Measuring success

Hybrid contests are chronic, so performance metrics should track resilience rather than single incidents: sectoral time-to-patch; time to detect and contain intrusions; changes in public trust; reductions in coordinated inauthentic behaviour; and diversification indices for energy and technology supply chains. Publishing these metrics – at least in aggregate – builds accountability and sustains political will.

List of References

Chapter 1

Aronov, Nikita. "'Comrade Putin, you're a great scientist.' How pro-Kremlin scholars study "Russophobia" and justify war." *The Insider*, 27 March 2023. https://theins.ru/en/society/260453 .

Berger, J. M. *Extremism.* MIT Press, 2018.

Bertelsen, Olga. "A Blind Spit of Active Measures," in *Russian Active Measures: Yesterday, Today, Tomorrow*. Ibidem-Verlag, 2021.

Birstein, Vadim. *SMERSH: Stalin's Secret Weapon.* Biteback Publishing, 2013.

Bloomfield, Alan. "Time to move on: Reconceptualizing the strategic culture debate." *Contemporary security policy* 33, no. 3 (2012).

Bunde, Tobias, Sophie Eisentraut, and Leonard Schütte. *Munich Security Index 2025.* Munich Security Conference, 2025. https://securityconference.org/en/publications/munich-security-report-2025/munich-security-index-2025/.

Council of the European Union. "Russian hybrid threats: EU agrees first listings in response to destabilising activities against the EU, its member states and partners," Council of the European Union, 16 December 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/12/16/russian-hybrid-threats-eu-agrees-first-listings-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-partners/ .

Curanović, Alicja. *The sense of mission in Russian foreign policy: destined for greatness!.* Routledge, 2021.

DeBenedictis, Kent. *Russian 'hybrid warfare' and the annexation of Crimea: the modern application of Soviet political warfare*. Bloomsbury Publishing, 2022.

Directorate General for External Security. "Nos modes de recrutement [Our recruitment modes]." DGSE, accessed on 19 March 2025. https://www.dgse.gouv.fr/fr/le-recrutement/nous-rejoindre .

Droit, Emmanuel. *Les polices politiques du bloc de l'Est. À la recherche de l'Internationale tchékiste, 1955-1989* [The political polices of the East bloc. The search of the Chekist international, 1955-1989]. Gallimard, 2019.

Duncan, Peter. *Russian messianism: third Rome, revolution, communism and after.* Routledge, 2002.

Edwards, Charlie. "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure." *IISS*, 19 August 2025. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/ .

European External Action Service. "3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the architecture of FIMI operations." EEAS, 19 March 2025. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

EUvsDisinformation. "DISINFO: The West is trying to undermine the friendship between Central Asia and Russia." *EUvsDisinformation,* 8 August 2024. https://euvsdisinfo.eu/report/the-west-is-trying-to-undermine-the-friendship-between-central-asia-and-russia/ .

– . "DISINFO: Military exercise Defender Europe 2020 is an act of war against Russia." *EUvsDisinformation,* 4 February 2020. https://euvsdisinfo.eu/report/military-exercise-defender-europe-2020-war-against-russia/.

– . "DISINFO: EU cites zero facts about Russia's alleged disinformation on coronavirus." *EUvsDisinformation*, 28 April 2020. https://euvsdisinfo.eu/report/eu-cites-zero-facts-about-russias-alleged-disinformation-on-coronavirus/.

– . "DISINFO: The Europeans can't even buy food for the first time in 75 years, but the EU prefers to remain silent." *EUvsDisinformation*, 11 April 2020. https://euvsdisinfo.eu/report/the-europeans-can-not-buy-food-75-years-eu-remain-silent/.

Falkov, Yaacov. "Intelligence-Exalting Strategic Cultures: A Case Study of the Russian Approach." *Intelligence and National Security* 37, no. 1 (2021).

Fedor, Julie. *Russia and the cult of state security: the Chekist tradition, from Lenin to Putin*. Routledge, 2011.

Galeotti, Mark. *Russian political war: Moving beyond the hybrid*. Routledge, 2019.

Grozev, Christo, Roman Dobrokhotov, and Michael Weiss. "'Morality and ethics should play no part': Leaks reveal how Russia's foreign intelligence agency runs disinformation campaigns in the West." *The Insider*, 4 July 2024. https://theins.ru/en/politics/272870 .

Hosaka, Sanshiro. "Unfinished Business: 1991 as the End of the CPSU but Not of the KGB." *Demokratizatsiya: The Journal of Post-Soviet Democratization* 30, no. 4 (2022). https://muse.jhu.edu/pub/280/article/878555/summary.

Juurvee, Ivo. *The Resurrection of 'active Measures': Intelligence Services as a Part of Russia's Influencing Toolbox.* Hybrid CoE, 2018. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-7-the-resurrection-of-active-measures-intelligence-services-as-a-part-of-russias-influencing-toolbox/.

Klein, Yitzhak. "A theory of strategic culture." *Comparative strategy* 10, no. 1 (1991).

Knight, Amy. *Putin's Killers: The Kremlin and the Art of Political Assassination*. Biteback Publishing, 2019.

Kozovoï, Andreï. *Les Services secrets russes.* Tallandier, 2020.

Laine, Martin, and Anastasiia Morozova. "Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections." *VSquare,* 16 September 2024. https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/.

Lenin, Vladimir. "For The All-Russia Extraordinary Commission Staff." *Izvestia* 214, 10 November 1918. https://www.marxists.org/archive/lenin/works/1918/nov/07b.htm.

Mezhdunarodnaya Zhizn. "Нарышкин заявил о провалах США на постсоветском пространстве [Naryshkin spoke about the failures of the US in the post-Soviet space]." *Mezhdunarodnaya Zhizn*, 10 December 2024. https://interaffairs.ru/news/show/49295.

Mlechin, Leonid. "Из чекистов в неодворяне [From Chekists to neo-nobility]." *Kommersant*, 4 December 2017. https://www.kommersant.ru/doc/3480134.

Mukhina, Olena. "Russia spends over $ 1 billion annually on disinformation campaigns." *Euromaidan Press*, 21 February 2025. https://euromaidanpress.com/2025/02/21/russia-spends-over-1-billion-annually-on-disinformation-campaigns/.

Novaya Gazeta Europe. "Say their names. Why remembering the victims of Soviet-era repression is more about Russia's future than its past." *Novaya Gazeta Europe*, 3 November 2024. https://novayagazeta.eu/articles/2024/11/03/say-their-names-en.

Reuters. "Up to 100 'suspicious incidents' in Europe can be attributed to Russia, Czech minister says," *Reuters,* 4 December 2024. https://www.reuters.com/world/europe/up-100-suspicious-incidents-europe-can-be-attributed-russia-czech-minister-says-2024-12-04/.

RIA Novosti. "Нарышкин прокомментировал ситуацию в Грузии [Naryshkin commented on the situation in Georgia]." *RIA Novosti*, 26 November 2024. https://ria.ru/20241126/naryshkin-1985728133.html.

Rid, Thomas. *Active measures: The secret history of disinformation and political warfare.* Profile Books, 2020.

Riehle, Kevin P. *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present*. National Intelligence Press, 2022.

Rossbach, Andreas . "Meet the Kremlin's keyboard warrior in Crimea." *Coda Story*, 29 May 2018. https://www.codastory.com/armed-conflict/meet-the-kremlins-keyboard-warrior-in-crimea/.

Rossiyskaya Gazeta. "Александр Бортников: ФСБ России свободна от политического влияния [Aleksandr Bortnikov: Russia's FSB is free from political influence]." *Rossiyskaya Gazeta,* 19 December 2017. https://rg.ru/2017/12/19/aleksandr-bortnikov-fsb-rossii-svobodna-ot-politicheskogo-vliianiia.html.
Secret Intelligence Service MI6. "Explore careers at SIS." Secret Intelligence Service MI6, accessed on 19 March 2025. https://www.sis.gov.uk/explore-careers.html.
Sherr, James. *Hard diplomacy and soft coercion: Russia's influence abroad*. Brookings Institution Press, 2013.
Snegovaya, Maria, and Alexander Lanoszka. "Reclaiming What Is Ours: Elite Continuity and Revanchism." *European Journal of International Security* (October 2024). https://www.cambridge.org/core/journals/european-journal-of-international-security/article/reclaiming-what-is-ours-elite-continuity-and-revanchism/3E0F188310117FE4E0D24FD5D494209A.
Snyder, Jack L. *The Soviet strategic culture: Implications for limited nuclear operations*. 1977.
Soldatov, Andrei, and Irina Borogan. "Dead Water: How the Russian Security Services' Paranoid Mindset Justifies the War." *Stockholm Centre for Eastern European Studies,* Guest Report 5 (2022). https://www.ui.se/globalassets/ui.se-eng/publications/sceeus/soldatov-borogan.pdf.
Walton, Calder. Spies: the epic intelligence war between east and west. Hachette UK, 2023.

Chapter 2

Andrew, Christopher, and Vasili Mitrokhin. *The Sword and the Shield*. 2001.
Arness, Stephen M. "Paper Mills and Fabrication." *Studies in Intelligence* 2. Central Intelligence Agency (1958). https://www.cia.gov/readingroom/docs/PAPER%20MILLS%20AND%20FABRICATION_0001.pdf.
Associated Press. "Russia-Estonia Sabotage Arson Ukraine." *AP News*, 4 July 2025. https://apnews.com/article/russia-estonia-sabotage-arson-ukraine-554442e8c139f4a1df4d2df78d76f7a4 .
– . "Poland-Russia Sabotage Ukraine War." *AP News*, 29 July 2025. https://apnews.com/article/poland-russia-sabotage-ukraine-war-4b3cfe0ea3a9d8f9c6147f3c573363dd.
– . "Poland-Russia-Ukraine Sabotage Court Prison." *AP News*, 21 February 2025. https://apnews.com/article/poland-russia-ukraine-sabotage-court-prison-19f84f9fb18083ae13acfb0b44274db0.
Badia i Dalmases, Francesc. "How Democracies Can Overcome Challenges of Hybrid Warfare and Disinformation." *Barcelona Centre for International Affairs* (September 2022). https://www.cidob.org/en/publications/how-democracies-can-overcome-challenges-hybrid-warfare-and-disinformation.
Baird, Frank B. Jr., and Richard E. Pipes. "Industrialization, 1929–34." Encyclopaedia Britannica, last updated on 26 October 2025. https://www.britannica.com/place/Soviet-Union/Industrialization-1929-34.
Bilal, Arsalan. "Russia's Hybrid War Against the West." *NATO Review*, 26 April 2024. https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html.
Central Intelligence Agency. "Kidnapping and assassination: Soviet executive action." *Studies in Intelligence* 19, no. 3 (1975). Approved for Release 26 January 2005. https://www.cia.gov/readingroom/document/cia-rdp78t03194a000400010014-6.
– . *RSFSR Criminal Code, 1956 Edition and Supplementary Material, Approved for Release*. Central Intelligence Agency (Freedom of Information Act Electronic Reading Room), 7 September 1999, https://www.cia.gov/readingroom/docs/CIA-RDP65-00756R000400010003-4.pdf.
– . *Soviet Active Measures and Disinformation. Declassified in Part – Sanitized Copy Approved for Release*. Central Intelligence Agency (Freedom of Information Act Electronic Reading Room), 6 February 2014. https://www.cia.gov/readingroom/docs/CIA-RDP89G00720R000500060008-2.pdf.
– . *Transmittal of Document Relative to the Macedonian Question in Yugoslavia*. Information Report, Central Intelligence Agency (Freedom of Information Act Electronic Reading Room),17 February 1950. https://www.cia.gov/readingroom/docs/CIA-RDP83-00415R001500100001-2.pdf.
Chambers, Whittaker. "Testimony before the House Committee on Un-American Activities, August 3, 1948." Famous Trials Project, UMKC School of Law, published online in 2003. https://law2.umkc.edu/faculty/projects/ftrials/hiss/8-3testimony.html.
Chivvis, Christopher S. *Understanding Russian "Hybrid Warfare" and What Can Be Done About It.* Testimony presented before the US House Armed Services Committee, RAND Corporation, 22 March 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.
Cull, Nicholas J., Vasily Gatov, Peter Pomerantsev, Anne Applebaum, and Alistair Shawcross. *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It – An Analytic History, with Lessons for the Present* (Final Report). London: LSE Consulting, October 2017. https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf.
Darczewska, Jolanta, and Piotr Żochowski. *Active Measures: Russia's Key Export*. Warsaw: Centre for Eastern Studies, June 2017. https://www.osw.waw.pl/sites/default/files/pw_64_ang_active-measures_net_0.pdf .
Deconinck, Carl. "Russia Trying to Sabotage European Railways, Says Czech Transport Minister." *Brussels Signal*, 5 April 2024. https://brusselssignal.eu/2024/04/russia-trying-to-sabotage-european-railways-says-czech-transport-minister/.
Dunton, Mark. "Confessions from the Cambridge Five: a file release from MI5." *The National Archives GOV.UK*, 14 January 2025. https://webarchive.nationalarchives.gov.uk/ukgwa/20250613153240/https://blog.nationalarchives.gov.uk/confessions-from-the-cambridge-five/ .
Encyclopaedia Britannica. "Third International." Encyclopaedia Britannica. Last updated on 21 August 2025. https://www.britannica.com/summary/Third-International.
ERR. "History: The 1924 December Coup Attempt in Estonia." *ERR News*, 30 November 2024. https://news.err.ee/1609534957/history-the-1924-december-coup-attempt-in-estonia.
– . "ISS: Russian Special Services Behind Attack on Estonian Minister's Car." *ERR,* 21 October 2024. https://news.err.ee/1609258853/iss-russian-special-services-behind-attack-on-estonian-minister-s-car .
European Commission. "EU Action to Address Energy Crisis." European Commission, last updated in 2024. https://commission.europa.eu/topics/energy/eu-action-address-energy-crisis_en .
Federal Bureau of Investigation. "The Neighborhood Spy: Zacharski-Bell Espionage Case." FBI, 3 June 2019. https://www.fbi.gov/news/stories/zacharski-bell-espionage-case-060319 .
– . "GRU Hackers: Destructive Malware and International Cyber Attacks." FBI Wanted List, last updated in 2020. https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks .
– . *Jay David Whittaker Chambers Part 01 (Final).* FBI Records: The Vault, 18 February 1949. https://vault.fbi.gov/Jay%20David%20Whittaker%20Chambers/Jay%20David%20Whittaker%20Chambers%20Part%2001%20%28Final%29/view .
– . *Solomon Adler Part 01.* FBI Records: The Vault, 26 March 1948. https://vault.fbi.gov/soloman-adler/Soloman%20Adler%20Part%2001.pdf.
Federation of American Scientists, National Counterintelligence Center. "Chapter 4: Counterintelligence Between the Wars." In *American Revolution to World War*. National Counterintelligence Center, 1996. https://irp.fas.org/ops/ci/docs/ci1/ch4b.htm.
Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." *In Moscow's Shadows*, 6 July 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

GlobalSecurity. "History of the Main Intelligence Administration (GRU)." GlobalSecurity.org. Last modified on 15 June 1996. https://www.globalsecurity.org/intell/world/russia/gru-history.htm.
Grierson, Jamie. "Romanian Man Arrested After DHL Warehouse Fire Caused by Suspected Russian Device." *The Guardian*, 9 April 2025. https://www.theguardian.com/uk-news/2025/apr/09/romanian-man-arrested-after-dhl-warehouse-fire-caused-by-suspected-russian-device.
Harris, James. "Historian James Harris Says Russian Archives Show We've Misunderstood Stalin." *History News Network*, 26 July 2016. https://www.historynewsnetwork.org/article/historian-james-harris-says-russian-archives-show.
Hedling, Elsa. *Social Identities and Democratic Vulnerabilities: Learning from Examples of Targeted Disinformation. Hybrid CoE Paper 24*. Helsinki: European Centre of Excellence for Countering Hybrid Threats, April 2025. https://www.hybridcoe.fi/wp-content/uploads/2025/04/20250415-Hybrid_CoE_Paper-24-WEB.pdf.
Irdi, Beniamino. "Hybrid Threats and Modern Political Warfare: The Architecture of Cross-Domain Conflict." *Jamestown Foundation*, 2 May 2025. https://jamestown.org/program/hybrid-threats-and-modern-political-warfare-the-architecture-of-cross-domain-conflict/.
Jakson, Heiki, James Brendan Byrne, Emanuele Nicola Cecchetti, Jan Ciampor, Jaroslav Hajek, Maximilian Hausler, and Kateryna Dubrova, *Energy in Irregular Warfare*. Vilnius: NATO Energy Security Centre of Excellence, 30 May 2017. https://www.enseccoe.org/wp-content/uploads/2024/04/irregular_warfare_176x250mm_20170526.pdf.
Jones, Seth G. "Russia's Shadow War Against the West." *Center for Strategic and International Studies*, 18 March 2025. https://www.csis.org/analysis/russias-shadow-war-against-west.
Lin, Herb. *Protecting Democracy in an Era of Cyber Information War.* Hoover Institution, 2018. https://www.hoover.org/research/protecting-democracy-era-cyber-information-war.
LRT. "Investigators: Russian GRU Behind Vandalising Lithuanian Partisan Leader's Monument." *LRT News*, 14 May 2024. https://www.lrt.lt/en/news-in-english/19/2601081/investigators-russian-gru-behind-vandalising-lithuanian-partisan-leader-s-monument.
MI5. "Klaus Fuchs." MI5 – The Security Service, last updated in 2025. https://www.mi5.gov.uk/history/the-cold-war/klaus-fuchs .
Michigan State University. "The Shakhty Trial." In *Seventeen Moments in Soviet History*. Michigan State University, 1928. https://soviethistory.msu.edu/?s=the+shakhty+trial .
Mitrokhin, Vasiliy (ed). *KGB Lexicon: The Soviet Intelligence Officer's Handbook*. London: Frank Cass, 2002. https://api.pageplace.de/preview/DT0400.9781136343445_A26886479/preview-9781136343445_A26886479.pdf.
National Cyber Security Centre. "NCSC Supports Sandworm Advisory." NCSC, 9 October 2020. https://www.ncsc.gov.uk/news/ncsc-supports-sandworm-advisory.
Parliament. House of Commons. *Russia No. 2 (1927). Documents illustrating the Hostile Activities of the Soviet Government and Third International against Great Britain*. His Majesty's Stationery Office, 1927. https://cdm21047.contentdm.oclc.org/digital/collection/russian/id/1519.
Paul, Amanda. "Hybrid Storm Rising: Russia and China's Axis Against Democracy." *European Policy Centre*, 2 May 2025. https://www.epc.eu/publication/Hybrid-storm-rising-Russia-and-Chinas-axis-against-democracy-64b158/.
Pavlova, Veneta. "Ninety Years Since the Bomb Attack on St. Nedelya Church." *Radio Bulgaria*, 16 April 2015. https://bnr.bg/en/post/100546082/ninety-years-since-the-bomb-attack-on-st-nedelya-church.
Plokhii, Serhii. "The Man with the Poison Gun: Q&A." Harvard Ukrainian Research Institute, 7 February 2017. https://www.huri.harvard.edu/news/man-poison-gun-qa-serhii-plokhii.
Reuters. "Germany Says It Won't Be Cowed by Russia After Reported Plot to Kill Rheinmetall CEO." *Reuters,* 12 July 2024. https://www.reuters.com/world/europe/germany-says-it-wont-be-cowed-by-russia-after-reported-plot-kill-rheinmetall-ceo-2024-07-12/.
– . "Rail Northern Germany Standstill Due to Technical Issue." *Reuters,* 8 October 2022. https://www.reuters.com/world/europe/rail-northern-germany-standstill-due-technical-issue-2022-10-08/.
Reynaud, Florian, Damien Leloup, and Antoine Albertini. "Coffins at the Eiffel Tower: Suspicions point to another case of Russian interference." *LeMonde*, 3 June 2024. https://www.lemonde.fr/en/pixels/article/2024/06/03/coffins-at-the-eiffel-tower-suspicions-point-to-another-case-of-russian-interference_6673608_13.html.
Richterova, Daniela. "The Long Shadow of Soviet Sabotage Doctrine?." *War on the Rocks*, 19 August 2024. https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/.
Rosenbach, Eric, and Katherine Mansted, *Can Democracy Survive in the Information Age?.* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, October 2018. https://www.belfercenter.org/publication/can-democracy-survive-information-age.
School of International and Public Affairs. "NotPetya: A Columbia University Case Study." *SIPA*-21-022.1, Columbia University (2021). https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf.
Strobel, Warren P., and Daniel Michaels. "Russia Plotted to Attack U.S. Planes With Incendiary Devices." *Wall Street Journal*, 8 April 2025. https://www.wsj.com/world/russia-plot-us-planes-incendiary-devices-de3b8c0a.
TIME. "Espionage: A Poor Devil." *TIME,* 26 October 1962. https://time.com/archive/6812167/espionage-a-poor-devil/.
Treverton, Gregory F. *Addressing Hybrid Threats.* Helsinki: European Centre of Excellence for Countering Hybrid Threats, July 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf.
US Congress, Office of Technology Assessment, *Technology and Soviet Energy Availability*. Washington, DC: U.S. Government Printing Office, June 1979. https://ota.fas.org/reports/7918.pdf .
US Department of Justice. "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere." Office of Public Affairs, 4 September 2024. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.
– . "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and International Cyber Attacks." Office of Public Affairs, 19 October 2020. https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.
US Department of the Treasury. "Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations." Press Release. US Department of the Treasury, 4 September 2024. https://home.treasury.gov/news/press-releases/jy2559.
UK Government. "UK Condemns Russia's GRU over Georgia Cyber Attacks." GOV.UK, 4 October 2019. https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.
University of Warwick. *The ARCOS Raid and the Break in Anglo-Soviet Relations, 1927*. Modern Records Centre, University of Warwick, 2011. https://warwick.ac.uk/services/library/mrc/collections/digital/russia/arcos/.
Weinstein, Allen. "IV The Ware Group and the New Deal." In *Perjury: The Hiss-Chambers Case*. Maryland State Archives Document, October 1995. https://msa.maryland.gov/megafile/ecp/10/214/pdf/00050004.pdf .
Weiss, Holger. *A Global Radical Waterfront: The International Propaganda Committee of Transport Workers and the International of Seamen and Harbour Workers, 1921–1937.* Leiden; Boston: Brill, 7 June 2021. https://brill.com/downloadpdf/display/book/9789004463288/BP000005.pdf.
Welfelt, Judy. "From the Editor." *Fairmount Folio: Journal of History* 13 (2011), 19 April 2016. https://journals.wichita.edu/index.php/ff/article/view/131.

RECENT ICDS PUBLICATIONS

REPORTS

Klyszcz, Ivan U.K. ***Russia and the Red Sea since 2022: The Wartime Engagements of an Aspiring Major Power***. November 2025.

Gretskiy, Igor. ***Not Quite Agents of Change: Russian Anti-War Grassroots Initiatives in Europe***. October 2025.

Blockmans, Steven, Butrint Berisha. ***From Stalemate to Solution: Rethinking EU Approaches to Bilateral Disputes in the Context of Enlargement***, October 2024.

Hosaka, Sanshiro, Toomas Hanso. ***Between Giants: Central Asia Balancing China, Russia, and the Rest***. September 2025.

Jermalavičius, Tomas, Henry Rõigas, Oleksandr Sukhodolia, and Dmitri Teperik. ***The Staying Power of Ukrainian Lights. Lessons of Wartime Resilience of the Electricity Sector***. May 2025.

Arjakas, Merili, Kai Kaarelson, Solveig Niitra, Hille Hanso, Ivan U.K. Lyszcz. ***Eesti roll muutuvas rahvusvahelise arengukoostöö arhitektuuris*** [Estonia's Role In the Changing Architecture of International Development Cooperation]. March 2025.

Klyszcz, Ivan U.K., Tony Lawrence, Eric Chan, Jyun-yi Lee. ***Deterrence and Hybrid Warfare: Lessons from Russia's War in Ukraine for Taiwan and the Nordic-Baltic Regio***n. February 2025.

POLICY PAPERS

Kallioniemi, Pekka. "**Beyond Defence: A Proactive Strategy for the West in the Information Domain**." November 2025.

Hall, Eric. "**Europe's Forthcoming Sahel Strategy: A Limited Role in a Multipolar Region**." October 2025.

Lawrence, Tony, Niklas Granholm, Björn Ottosson, and Igor Schvede. "**Hybrid and High-End Warfare in the Baltic Sea Region: Safeguarding our Maritime Domain**." September 2025.

Alatalu, Siim. "**Cyber Solidarity in the Making: Is the EU Stepping into NATO's Blind Spot?**" August 2025.

Lawrence, Tony, Felix Gasper, and Dick Zandee. "**Defending Europe's Skies: Challenges and Prospects**." May 2025.

Klyszcz, Ivan U.K."**Distance is Not a Shield. Russia's Transnational Repression in Wartime**," May 2025.

Praks, Henrik. "**Russia's Hybrid Attacks in Europe: From Deterrence to Attribution to Response.**" April 2025.

ANALYSES

Hanso, Toomas. "**More Than Meets the AI: China's Data Centre Strategy**." November 2025.

Mikelsaar, Anniki. "**Ruptures at the Top of the World: High North Network Infrastructure Protection**." September 2025.

Gasper, Felix, Lukas Mugele. "**Forward Defence in the Cold War.**" August 2025.

Leveque, Arthur, and Justin Leveque. "**Foreign Interference in Distant Territories: French Territories on Azerbaijan's, Russia's, and China's radars**." August 2025.

Larsen, Henrik. "**Toward a Europeanised NATO**." June 2025.

Hanso, Toomas. "**Central Asia's New Railways: Russia's Pain, China's Gain**." March 2025.

BRIEFS

Heap, Ben, Sahaidachnyi Security Center, Hennadiy Maksak, and Laurynas Jonavičius. ***Russia's War in Ukraine Series***. October 2025.

Klyszcz, Ivan U. K., "**Russia and the Red Sea since 2022: Militarised Foreign Policy or Strategy of Conflict?**." September 2025.

Nazarov, Mykola. "**Ukrainian War Refugees in Estonia: Sociodemographic Portrait and Support Policies**." September 2025.

Hosaka, Sanshiro. "**Trump-Brokered Azerbaijan-Armenia Peace Deal: Breakthrough or Another Geopolitical Conundrum?**" August 2025.

Kimoita, Stephen. "**Kenya's Foreign Policy Towards Europe and Estonia**." July 2025.

Huminski, Joshua C., Tony Lawrence, Marianne Paire, Nele Loorents, Katarzyna Zysk, Felix Gasper, ***Hague Summit Series***. June 2025.

Cordet, Maxime, Marianne Paire, and Mihai Chihaia. **EU Defence Series**. May 2025.

All ICDS publications are available from https://icds.ee/category/publications/.

ICDS.Tallinn
@ICDS-TALLINN.BSKY.SOCIAL
@ICDS _ Tallinn
ICDS-Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-0529
ISBN 978-9916-709-57-3 (print)
ISBN 978-9916-709-58-0 (pdf)